[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 17/30
G06F 12/00

[12]发明专利申请公开说明书

[21]申请号 00134899.X

[43]公开日 2001年7月11日

[11]公开号 CN 1303065A

[22]申请日 2000.9.30 [21]申请号 00134899.X

[30]优先权

[32]1999.9.30 [33]JP [31]279208/1999

[32]1999.10.19 [33]JP [31]296669/1999

[32]2000.7.25 [33]JP [31]224534/2000

[71]申请人 卡西欧计算机株式会社

地址 日本东京

[72]发明人 佐藤诚 竹田恒治

森润二 黑泽和大

[74]专利代理机构 永新专利商标代理有限公司

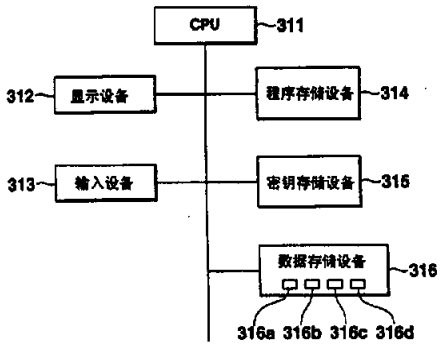
代理人 蹇 炜

权利要求书6页 说明书63页 附图页数35页

[54]发明名称 数据库管理装置和加密/解密系统

[57]摘要

在一数据库中,频繁检索的列项用公用密钥加密,而其他列是使 用指定的行密钥加密的。由此检索处理能以高速进行,并能提高安全 性。另外,通过假定要加密的原文是位串,并用随机位串执行一二进 制运算来加密数据库的行和列。随机位串的获得是通过定义1个字和多个字的预定位长作为多维向量的分量,用非线性函数顺序产生多维 向量而获得的。



ISSN1008-4274

00.10.29

权 利 要 求 书

1.一种数据库管理装置，包括：

一加密密钥规范单元，规定是用列项中公用的列密钥还是用相关于各行的行密钥来对数据库中一列项数据进行加密；

一加密单元，用所说的加密密钥规范单元指定的密钥加密数据库的各列项；

一存储单元，将由所说的加密单元加密的数据库存储在存储器中。

2.根据权利要求 1 的数据库管理装置，其中还包括：

一数据库搜索单元，当检索使用公用行密钥加密的列项时，使用预定列项中公用行密钥加密检索输入数据，将加密的检索数据与存储在存储器中加密数据库的各项数据进行比较，执行检索处理。

3.根据权利要求 1 的数据库管理装置，其中所说的加密单元使用相关于各行指定的行密钥和相应列项中的公用列密钥的组合加密一预定列项的数据。

4.根据权利要求 1 的数据库管理装置，其中所说加密单元基于预定函数在一多维空间产生顺序的向量，使用作为加密系统函数常数的行密钥和列密钥加密一数据库，该加密系统采用作为加密密钥流的向量元素。

5.一种数据库系统，包括，第一信息终端，该第一信息终端包含一数据库；和请求该第一信息终端搜索该数据库的第二信息终端；并通过网络连接该第一和第二信息终端，其中：

在该第一信息终端侧，该数据库列项的第一类型数据使用列项中公用列密钥加密，列项的第二类型数据使用相关于各行的行密钥加密；

当第二信息终端请求搜索相关于列项的第一类型数据库时，检索

输入数据使用列项中公用列密钥加密，加密的检索数据通过网络传送到第一信息终端；和

在第一信息终端侧，加密数据库使用检索数据搜索；作为搜索结果获得的加密数据通过网络返回到第二信息终端。

6.一种管理数据库的数据库管理装置，其中数据使用预定列项中公用列密钥被加密，该装置包括：

一加密单元，当从预定列项检索数据时使用列密钥加密输入检索数据；和

检索单元通过将加密的检索数据与加密数据库各项数据相比较进行数据的检索。

7.根据权利要求 1 的数据库管理装置，其中包括：

一原文数据获取单元，用于获取要加密的原文；

一向量产生单元，使用由至少该列密钥或一行密钥确定的一函数顺序产生在 n(n≥1)维空间闭合区定义的向量；和

一逻辑运算单元，使用由所说原文数据获取单元获取的原文数据和由所说向量产生单元产生的向量元素按位单元进行一逻辑运算，产生加密数据。

8.一种计算机可读存储媒体，用于存储控制计算机完成处理过程的程序，包括：使用列项中公用密钥来加密数据库列项的第一类型数据，和使用相关于各行指定的行密钥来加密列项第二类型数据；和

搜索作为加密函数的结果获得的加密数据库。

9.一种计算机可读存储媒体，用于存储控制计算机完成处理过程的程序，包括：

当从预定列项检索数据时使用列密钥来加密输入检索数据；和

通过将加密检索数据与加密数据库各项数据相比较检索数据。

10.一种数据库管理装置，包括：

第一加密单元，使用列项中公用列密钥加密数据库列项第一类型

数据，和使用相关于各行的行密钥加密列项第二类型数据；

第二加密单元，使用各行中另外的公用密钥加密该行密钥，该行密钥是在由所说第一加密单元加密数据库列项的第二类型数据中使用的；和

存储单元，将所说第一加密单元加密的数据库和所第二加密单元加密的行密钥存储在存储器中。

11.根据权利要求 10 的数据库管理装置，其中所说行密钥由指定给所说数据库各行的行数和一随机数产生。

12.根据权利要求 10 的数据库管理装置，其中包括：

向量产生单元，使用由该数据库管理装置中各密钥确定的函数顺序产生在 n(n≥1)维空间闭合区定义的向量；和

逻辑运算单元，使用由所说原文数据获取单元获取的原文数据和由所说向量产生单元产生的向量分量按位单元进行逻辑运算，产生加密数据。

13.一种数据库系统，包括一第一终端单元，用于管理一数据库；和一第二终端单元，它独立于第一终端单元，用于搜索该数据库，其中：

在该第一终端单元侧，该数据库被加密并把加密数据库存储在便携式存储媒体中，而该存储媒体是被分配的；和

在该第二终端单元侧，使用所说被分配的存储媒体搜索加密数据库，解密及显示作为搜索结果获取的数据。

14.根据权利要求 13 的系统，其中：

所说第一终端单元使用列项中公用列密钥加密数据库列项第一类型数据，使用指定给各行的列密钥加密列项的第二类型数据，使用行中另一公用密钥加密行密钥；和

所说加密数据库与加密后的行密钥存储在存储媒体中。

15.根据权利要求 13 的系统，其中

所说存储媒体用于存储在所说第一终端单元加密的数据库，和存储用于搜索加密数据库的预定程序。

16.一种计算机可读存储媒体，用于存储控制计算机完成处理过程的程序，包括：

使用列项中公用列密钥来加密数据库列项第一类型数据，和使用相关于各行指定的行密钥来加密列项第二类型数据；和

使用行中另外的公用密钥加密行密钥，该行密钥是由所说第一加密函数在加密数据库列项第二类型数据时使用的。

17.一种加密系统，包括：

旋转矩阵产生单元，使用一向量的各分量和取决于一参数组 p 的角 Ω_n 产生用于旋转在 n(n≥1)维空间闭合区定义的该向量的 n 维旋转矩阵 $R_n(\Omega_n)$，以使能包含（n-1）维旋转矩阵 $R_{n-1}(\Omega_{n-1})$ 作为（n-1）维小矩阵；

向量产生单元，用于产生一向量 r_j，使得用包含至少该旋转矩阵 $R_n(\Omega_n)$的非线性函数顺序产生的向量 r_j（j≥0)在 n 维空间不互相匹配；

二进制运算单元，通过使用原文数据和由所说向量产生单元产生的向量 r_j 的各分量进行二进制运算产生加密数据。

18.根据权利要求 17 的系统，其中：

所说向量产生单元的非线性函数是一个包含用于一旋转向量的空间平移的固定向量的函数，而所说向量产生单元顺序产生向量以使产生的向量不能互相匹配。

19.根据权利要求 17 的系统，其中：

所说向量产生单元使用的所说 n 维旋转矩阵 $R_n(\Omega_n)$是由 n 维旋转矩阵的乘积产生的，该 n 维旋转矩阵是通过改变相应于(n-1)维旋转矩阵 $R_{n-1}(\Omega_{n-1})$的(n-1)维小矩阵的引入位置变化而产生的。

20.根据权利要求 17 的系统，其中：

所说二进制运算（op）指示在执行一加扰运算 S 后执行异或逻辑和运算（XOR），由下式表示

$op=XOR \cdot S$

21.根据权利要求 17 的系统，其中：

加密数据 C_j 是通过对原文数据 M_j 和一向量进行的二进制运算产生的，该向量是通过由所说向量产生单元使用的非线性函数产生的第 j 个（j-th）向量 r_j 和产生的第 j-1 个加密数据 C_{j-1} 的检验和 Σ_{j-1} 进行的二进制运算获取的。

22.一解密系统，包括：

一向量产生单元，用于产生向量 r_j 以使由一非线性函数顺序产生的向量 r_j 在 n 维空间互相不匹配，该非线性函数包含至少一 n 维旋转矩阵 $R_n(\Omega_n)$，该矩阵用一定义在 n 维空间闭合区的向量的各分量和取决于参数组 p 的角 Ω_n 来旋转该向量；

一逆二进制运算单元，用于接收来自加密侧的加密数据，该加密数据是通过对原文数据和由与所说向量产生单元类似方法产生的向量 r_j 的分量进行的二进制运算产生的；且通过使用所说向量产生单元产生的向量 r_j 和该加密数据，执行相应于该二进制运算相反运算的二进制逆运算来解密出原文数据。

23.根据权利要求 21 的系统，其中

所说旋转矩阵 $R_n(\Omega_n)$ 是由所说旋转矩阵产生单元产生的。

24.根据权利要求 21 的系统，其中

由所说向量产生单元使用的非线性函数是包含用于旋转向量的空间平移的固定向量的函数，而所说向量产生单元顺序产生向量，以使这些向量不互相匹配。

25.根据权利要求 21 的系统，其中

由所说向量产生单元使用的 n 维旋转矩阵 $R_n(\Omega_n)$ 是通过改变相应于(n-1)维旋转矩阵 $R_{n-1}(\Omega_{n-1})$ 的(n-1)维小矩阵的引入位置产生的 n

维旋转矩阵的乘积产生的。

26.根据权利要求 21 的系统，基中

所说二进制运算（op）指示执行一加扰运算 S 后执行异或逻辑和运算（XOR），由下式表示

$op = XOR \cdot S$

所说逆二进制运算（op^{-1}）指示执行异或逻辑和（XOR）运算后执行相反于加扰运算 S 的逆运算 S^{-1}，由下式表示

$op^{-1} = S^{-1}\ XOR$

27.根据权利要求 26 的系统，其中

生成第 j-1 个接收的加密数据 C_{j-1} 的检验和 Σ_{j-1}，并且二进制运算是使用该生成结果和所说向量产生单元所用的非线性函数产生的向量 r_j 来完成的，而逆二进制运算是使用该二进制运算产生的向量与接收的第 j 个加密数据 C_j 进行的，由此解密原文数据 M_j。

28.一种向量产生系统，用于数据库管理装置和加密 / 解密系统中，其中

当产生用于以一定义在 n 维空间闭合区的一向量的各分量和取决于一参数组 p 的角来旋转该向量的一 n 维旋转矩阵 R 时，多个小维数旋转矩阵作为对角块（diagonalblock）设置，而作为零元素产生的伪旋转矩阵 Q 用在其余部分。

29.根据权利要求 28 的系统，其中

当产生用于以一定义在 n 维空间闭合区的一向量的各分量和取决于一参数组 p 的角来旋转该向量的一 n 维旋转矩阵 R 时，多个小维数旋转矩阵作为对角块（diagonal block）设置，而将通过用置换矩阵 S 来对作为 0 元素生成的一伪旋转矩阵进行式 $P=S\cdot Q\cdot S^T$ 所表示的类似的变换而形成的矩阵 P 用于其余的部分。

00.10.29

说　　明　　书

数据库管理装置和加密／解密系统

本发明涉及一用于执行加密的数据通信系统中的加密／解密系统，和一用于加密和管理数据库的数据库管理装置。

例如在广大一般用户使用的计算机和网络信息系统中，存在着一个严重的问题，即某些有预谋的用户非法存取和修改信息。因此加密技术已经被广泛使用作为有效对策。公知的加密技术详细披露在下述文献。

见 ACM 通信 21 卷 2 期（1978）P120，题目：获得数字签名和公钥密码的系统，麻省理工学院（MIT）计算机科学研究所和数学研究部作者 R.L.Rivest,A.Shamir 和 L.Adleman。

公开在这份文献中的加密方法普遍认为是一相当可靠的方法，涉及到一 RSA（公开密钥密码系统）方法，从该 RSA 推导的系统已经研制成用于签名的鉴别系统，应用于电子贸易系统中并且已实际投入使用。

该 RSA 方法基于分解素数的难度是一个公钥（非对称）加密系统，通过将引发的数据除以大整数得到余数获得密码文件。RSA 方法的特点是难于从两个原始素数的乘积中找出两个素数（p 和 q）。即使能查出两个素数的乘积也难于找出 p 和 q 或难于估计该解码操作。上述 RSA 方法当加密密钥的数据位长足够长时在某种意义上实用。为了保证可靠性通常用的加密密钥数据为 256 位长。但在某种情况下，它还不够长，实际细究起来需要 512 或 1024 位的数据长度。然而因为数据长度受计算机运算精度和运算速度限制，长的比特位是无形的。

也就是说用 RSA 方法和用从 RSA 推导出的加密方法存在着问

题，这些方法的可靠性受计算机特性限制，另外，该方法用于基于加密密钥位长变化的鉴别系统的可靠性等试验时需要显著变化。

此外，该数据库管理装置必须加密和必须管理存储于其中的数据库以保证数据的安全。

为了提高安全性可执行更复杂的加密处理，但也需要长时间进行运算。

一个数据库中包含大量数据，在数据检索过程中，相关于一特定项和与已知条件符合的数据从大量数据中选择，而包含有与该条件符合的项数据的记录（行数据）被输出。因此在处理大量数据的数据检索系统中延长运算时间会造成系统特性降低。

如上所述含有机密数据的数据库需要保证其安全性。为提高安全性，加密处理数据库，该处理如出现问题会降低数据库的可用性。

按惯例，当加密数据库时，通常用例如用口令等产生的固定加密密钥加密全部目标文件。

但如上所述，因为加密处理已经根据惯用系统使用固定加密密钥被执行。每个数据项的安全级被平均。此外，当存在含有相同的数据的多个项目时，输出相同的加密结果，由此产生了解密该加密密钥的可能性。

本发明目的在于提供一加密／解密装置，该装置能够在没有精密运算的结果的情况下进行加密处理。且能实现一通用的加密／解密处理，该处理具有高可靠性和易于相加和变化一应用。

本发明另一目的是提供一数据库管理装置，该装置能够保证数据库安全并快速的检索数据。

本发明又一目的是提供一数据库管理装置，能够加密数据库中的指定数据项使其具有比其他数据项更高的安全性。本发明的数据库管理装置加密检索处理中的一列项数据，该检索过程使用了通常用在该列项的列密钥和使用指定给每行的行密钥加密其他列项。

00.10.29

本发明的加密设备包括：原文件数据获得单元，用于获得将要加密的原文件数据；向量产生单元，用于顺序产生限定在 n(n≥1)维空间封闭区中的向量；和一逻辑运算单元，用于通过逻辑运算产生加密的数据，该运算是在由向量产生单元产生的向量元素和原文件获得单元获得的原文件数据基础上进行的。另方面本发明的解密设备也包括向量产生单元，和逆逻辑运算单元，它使用密码文件通过该逻辑运算的逆运算解码原文件数据。

本发明的数据库管理装置，在加密处理时使用本发明的加密设备，而当把密码文件数据解密为原文件数据时使用本发明的解密设备。

本发明的加密系统包括：向量产生单元，用于由 n(n≥1)维空间封闭区中定义的各向量元素和由参数组 p 确定的角 Ω_n 产生向量 r_j，产生向量 r_j 采用了这样的方法，使非线性函数顺序产生的各向量 r_j (j≥0)在 n 维空间互相不匹配，该非线性函数包括：用于旋转该向量的至少 n 维旋转矩阵；和一个二进制运算单元，采用原文件数据和由向量产生单元产生的向量 r_j 的二进制运算产生加密的数据。

本发明的解密系统包括：向量产生单元，用于由 n(n≥1)维空间封闭区中定义的各向量元素和由参数组 p 确定的角 Ω_n 产生向量 r_j，产生向量 r_j 采用了这样的方法。使非线性函数产生顺序的各向量 r_j (j≥0)在 n 维空间互相不匹配，该非线性函数包括：用于旋转该向量的至少 n 维旋转矩阵 $R_n(\Omega_n)$；一逆二进制运算单元，用于接收原文件数据的二进制运算产生的加密数据和类似于向量产生单元的方法产生的向量 r_j 元素，对应于使用向量产生单元产生的向量 r_j 和该加密的数据的二进制运算的逆运算按逆二进制运算解密该原文件。

按照上述配置，在 n(n≥1)维空间封闭区中定义的向量顺序地产生，并且按照将要加密的原文件数据和向量元素的一逻辑运算产生密码文件数据。

由此，通过使用多维向量元素加密原文件数据，在没有经过例如RSA 方法的精密运算的情况下也能进行加密处理和实现一可靠通用的加密／解密处理，该处理容易相加和变化一应用。

本发明数据管理装置包括：加密单元，用于使用列项中公用的列密钥(column key)加密数据库预定列项的数据，和使用指定给各行（row）的列密钥加密其它列数据；还有一存储单元，用于储存加密单元加密的数据库。

按照该配置，当加密数据库时，通过向各行赋值不同的密钥能提高安全性。当执行检索处理时，使用预定列项中公用的列密钥加密检索输入数据，将加密的检索数据的项数据和加密的数据库的数据相比较实现高速检索处理。

此外，使用指定给各行的行密钥和列项中公用的列密钥的组合通过对列项的数据而不是检索处理中用的列项进行加密能进一步提高安全性。

另外，数据库可存储在不同的位置以产生数据库系统使请求的一检索处理能通过一网络从不同的信息终端发出。在这种情况下，预定列项的数据（用在检索处理中的列项）使用列项中公用的列密钥加密，和其他列项的数据使用指定给各行的行密钥加密。当检索数据库的请求从另一信息终端发出时，使用列项中公用的列密钥加密检索的数据，并通过网络传送加密的检索数据。通过接收该检索的数据，检索加密数据库的处理能被执行，且作为检索结果获得的加密数据通过网络返回到信息终端。因此，数据在加密状态下不断传送，数据库的安全得到了保证。

当加密数据库时，本发明的数据库管理装置用列项中公用的列密钥加密检索处理时用的列项数据，用指定给各行的行密钥与用行中公用的另外密钥又加密的行密钥加密要求高安全性的其他列项的数据。

实际上，本发明的数据库管理装置包括：一第一加密单元，用列项中公用的列密钥加密数据库预定列项的数据，和用指定给各行的行密钥加密其他列项的数据；一第二加密单元，用于加密该行密钥，该行密钥用于加密第一加密单元使用各行中公用的另外密钥来加密的数据库的其他列项数据；和存储单元，用于将由第一加密单元加密的数据库与由第二加密单元加密的行密钥一起储存。

按照该配置，当加密数据库时，列项的数据而非检索处理中用的预定列项数据能使用相关于各行的不同密钥加密，使得对于列项中相同值的数据能够获得不同值的加密结果，并且利用另外密钥对该密钥（行密钥）进行再加密，然后对该密钥进行复杂的解密可实现高安全性。该行密钥用于加密该些列项。

而且当使用赋值给数据库各行的行数和使该密钥的加密更困难的随机数产生行密钥时，能成功地提高安全性。

此外一数据库系统能由第一终端设备与第二终端设备构成，第一终端设备用于管理数据库；第二终端设备独立于第一终端设备，用于检索该数据库。

在数据库中，第一终端设备加密该数据库，将已加密的数据库存储在存储媒体中，并且分配存储媒体，第二终端设备检索储存在分配媒体中已存储的加密数据库中的数据，解密所获得的数据作为该检索结果，并显示该结果数据。在此情况下，数据库中预定列项的数据用列项中公用的列密钥加密，其它列项的数据用指定给各行的行密钥加密，而该行密钥用列中公用的另外密钥加密，由此将该数据库存储在存储媒体中，并在安全得到成功保证下分配该储存介质。

图 1 说明本发明第一实施例的数据库管理装置的配置；

图 2 是由该数据库管理装置执行的数据库加密处理操作的流程图；

图 3A 和 3B 是由该数据库管理装置执行的数据库检索处理的操

作流程图；

图 4A 和 4B 是图 18A 步骤 P13 表示的检索处理实际操作的流程图；

图 5 是说明本发明数据库管理装置第一实施例的数据库配置；图 5(a)说明加密前的该状态；图 5(b)说明加密后的该状态；和图 5(c)说明解密后的该状态。

图 6 说明本发明数据库管理装置第一实施例的列密钥和行密钥的配置；

图 7 说明本发明数据库管理装置第二实施例的数据库配置；图 7(a)说明加密前的状态；图 7(b)说明加密后的状态；7(c)说明解密后的状态；

图 8 说明本发明数据库管理装置第二实施例的组合密钥的配置；

图 9 是本发明数据库管理装置第三实施例的数据库系统配置的方框图；

图 10 说明本发明第四实施例的数据管理装置；

图 11 是数据库管理装置功能配置方框图；

图 12 说明数据库管理装置中用于设置一基本密钥的对话的配置；

图 13 说明数据库管理装置中基本密钥参数表的一个例子；

图 14 说明数据库管理装置中用于设定密钥规范对话的配置；

图 15 说明数据库管理装置中密钥规范表中条目（entry）的一个例子；

图 16 说明在数据管理装置中加密和解密该数据库时的数据流；

图 17A 和 17B 是由数据库管理装置执行的数据库加密处理的操作流程图；

图 18A 和 18B 是由数据库管理装置执行的数据库检索处理的操

作流程图；

图 19A 和 19B 是说明在图 18A 中的步骤 P13 中检索处理的实际操作流程图；

图 20 说明数据库管理装置中数据库的配置；图 20(a)说明加密前的状态；图 20(b)说明加密后的状态；图 20(c)说明解密后的状态；

图 21 是本发明数据管理装置第五实施例的数据库配置的方框图；

图 22 说明数据库系统中使用的存储媒体的数据内容；

图 23 说明根据本发明一实施例，用于完成被加密的数据通信的系统配置；

图 24 是在该系统中安全设备 PC 电路配置方框图；

图 25 说明安全设备的数据库配置；

图 26 是在该施例中当做出一用户条目时 PC 和安全设备的处理操作流程图；

图 27 是在该实施例中加密数据时 PC 和安全处理操作的流程图；

图 28A 和 28B 是在该实施例中加密和解密处理操作的流程图；

图 29 说明本发明使用多维向量的加密操作的方法；

图 30 说明用于表示本发明加密／解密系统原理的系统配置；

图 31 说明图 8 中表示的设备 110 和 112 的内部功能的一个例子；

图 32 是产生多维向量的处理流程图；

图 33 是使用产生多维向量的该处理的加密／解密流程图；

图 34 是本发明一实施例的解密处理的流程图；

图 35 是本发明一实施例的产生了 3 维向量 r_j 的处理的流程图；

图 36 是本发明一实施例产生 n 维旋转矩阵 $R_n(\Omega_n)$ 的处理的流程图；

00.10.29

图 37A 至 37C 说明本发明一实施例的三维向量的旋转操作流程图；

以下参考附图描述本发明的一实施例。

图 1 说明本发明数据管理装置的配置。

该装置包括按行和列的矩阵形式的数据库，该装置具有以下功能：加密和管理数据库，加密输入的检索数据，及根据加密的检索数据检索该数据库。该装置读出存储在例如磁盘等的存储媒体中的一程序，并由该程序控制计算机操作完成。

如图 1 所示，该装置包括：CPU311，显示设备 312，输入设备 313，程序存储设备 314，密钥存储设备 315，和数据存储设备 316。

CPU311 控制整个设备，读出存储在程序存储设备 314 中的程序，根据该程序执行各种处理。根据本实施例，CPU311 执行图 2 所示的数据库加密处理，及执行图 3A 到 4B 所示的数据库检索处理。

显示设备 312 是用于显示数据的设备，采用例如 LCD（液晶显示），CRT（阴极射线管）等。输入设备 313 是用于输入数据的设备，例如可以是键盘，鼠标等。

程序存储设备 314 包括：例如 ROM，RAM 等和存储该装置必须的程序，该装置需要例如数据库管理程序，加密程序等。

程序存储设备 314 还可包括除半导体存储器外的磁和光存储媒体。存储媒体包括便携式媒体，例如 CD－ROM 等和固定媒体，例如硬盘等。储存在存储媒体中的全部或部分程序能够从服务器的传输控制单元接收和通过例如网络等的传输媒体等从客户接收。存储媒体可以是设置在网络中的服务器的存储媒体。而且在程序通过例如网络电路等传输到该服务器和该客户后，可以设计将该程序装在服务器和客户的设备上。

密钥存储设备 315 包括：例如 RAM 等，当数据库加密时用于存储一密钥（行密钥和列密钥）。

数据存储设备 316 是用于存储该装置各种必须数据的设备，它包括：例如 RAM 或外部存储设备例如磁盘设备等。数据存储设备 316 提供用于存储数据库的数据库存储区 316a，用于存储当存储数据库时由操作员设置的信息（将要检索的项，非加密的项等）的加密设置信息存储区 316b，用于存储当检索数据库时由操作员设置的信息（目标列项，检索的字符串等）的检索设置信息存储区 316c，当数据库检索时提供用于存储比较字符串的一比较字符串存储区 316d。

在描述该装置操作以前，首先描述该装置使用的数据库加密方法。

当加密数据库时，如果把不同密钥用于各行（记录），解密一个密钥就会变得更困难，由此提高安全性。但是，因为加密的数据必须使用相关于各行的密钥解密或当检索数据库时输入的检索数据（关键词）必须使用相关于各行的密钥加密，这将花费长时间以获得检索结果，另一方面，如果数据库使用相关于各列的不同密钥加密，检索数据只使用一个相应于要检索的列项的密钥加密，由此能以高速检索一数据库。但是在相同列中存在相同数据时，会输出相同的加密结果，这样可能使该密钥被解密。

本发明的特点在于，当加密数据库时，使用公用列密钥（common column key）加密检索处理中频繁使用的列项数据，利用为各行赋值的不同密钥加密其他列项的数据。也就是说把不同密钥用于各行能提高安全性，并且通过使用一列密钥加密输入检索项的数据以及将该加密结果与数据库中加密的数据相比较能够实现高速检索处理。

图 5 示出本发明数据库管理装置第一实施例的配置；图 5(a)示出加密前的状态；图 5(b)示出加密后的状态；和图 5(c)示出解密后的状态。图 6 说明数据库管理装置第一实施例的列密钥和行密钥的配置。

如图 5(a)所示，该装置具有一行和列组成的矩阵。图 5(a)示出作为数据库的个人数据。该数据库有一记录包括了下列各项：‘编号’

‘姓名’‘体重’‘身高’‘年龄’和‘电话’。

该数据库使用列密钥和行密钥加密。即，当检索处理中频繁使用的列项包括‘姓名’‘州’，和‘年龄’时，该列项各行数据使用列项中公用列密钥例如‘苹果’‘桔子’‘柠檬’等加密，如图 6 所示，其他列项的各行数据‘体重’‘身高’和‘电话’使用指定给各行的密钥加密。

假定‘编号’这行不加密。所使用的行密钥有‘虎’，‘狗’，‘猫’，‘老鼠’，‘象’，‘母牛’，‘猪’，‘兔’，‘狮子’等。

这些列密钥和行密钥确定了一预定的非线性函数，加密（解密）处理通过该函数和用该函数产生的数学向量的二进制运算（逆二进制运算）进行。在此情况下，可按如下所述使用本发明的加密 / 解密系统。

图 5(b)说明使用列密钥和行密钥加密图 5(a)所示的数据库形成的结果。数据存储设备 316 的数据库存储区 316a 存储了图 5(b)所示状态的数据库。

当检索数据库时，使用与检索时所用的列项相对应的列密钥加密检索的数据，然后执行检索处理，例如当要检索‘州’中的‘佛罗里达’数据时，使用‘州’中的列密钥‘桔子’加密作为检索数据输入的‘佛罗里达’，于是获得‘h*/fDD’。为 h*/fDD 的数据从‘州’的列中的各行中检索出来。由此确定对应于‘编号 2’和‘编号 8’ 该数据存在。

此外，当把加密的数据库恢复为原始状态时，使用加密处理时用过的列密钥和行密钥。如图 5(b)所示当使用数据库加密处理时所用的列密钥和行密钥解密数据时，可获得如图 5（c）所示的原始数据。

该装置的操作描述如下。

加密数据库的处理（a）和检索数据库的处理（b）将分别进行描

述。用于实现图 2 到 4 流程的各种功能的程序以 CPU 可读程序代码形式存储在程序存储设备 314 的存储媒体。程序也能通过传输媒体，例如网络电路，传送。

(a) 加密数据库时：

图 2 是该装置执行数据库加密处理的流程图。图 5(a)说明存储在数据存储设备 316 的数据库存储区 316a 中的数据库的未加密状态。

首先，在数据库加密设定屏幕上，指定要加密的一个数据库（步骤 G11）。

然后，在数据库的列项中设定检索处理时所用的列项和不加密的列项（步骤 G12）。在图 20(a)所示的举例中，在检索处理时所用的列项是‘姓名’，‘州’，和‘年龄’，不加密的列项是‘编号’。设定的信息存储在数据存储设备 316 的加密设定信息存储区 316b 中。

然后确定加密数据库时所用的行密钥和列密钥（步骤 G13）。有关确定行密钥和列密钥的信息存储在密钥存储设备 315 中。

当上述设定操作执行后，顺序指定数据库中列项（步骤 G14），根据设定信息确定用于该列项的加密系统（步骤 15）。在此情况下，因为‘编号’列项在数据库中设定为非加密，不执行处理。即‘编号’项按照原来的数据不改变。

当指定的列项设定为检索处理所用的列项时，存储在密钥存储设备 315 中的该列项的公用列密钥被读出（步骤 G15 和 G16），该列项的各行数据用该列密钥加密（步骤 G17）。即，数据库中‘姓名’，‘州’和‘年龄’各项的各行用指定给各列的密钥例如‘苹果’，‘桔子’，‘柠檬’加密，如图 6 所示。

当指定的列项没有设定为检索处理所用的列项，也就是作为其它列项时，存储在密钥存储设备 315 中的与每行相应的行密钥被读出

（步骤 G15 和 G18），该列项的各行数据用特定行密钥加密（步骤 G19 和 G20），即数据库中“州”，“体重”，“身高”各列项的第 1，2，3，4，5，6，7，8 和 9 行数据分别用各自对应的行密钥‘老虎’，‘狗’，‘猫’，‘老鼠’，‘象’，‘母牛’，‘猪’，‘兔’，和‘狮子’来加密，如图 6 所示。

于是，对数据库的每个列项重复进行加密处理。当在所有列项的各行完成数据加密处理时，在数据存储设备 316 的数据库存储区 316a 改写加密的数据库。图 5(b)说明该状态。

(b) 检索数据库时:

图 3A 和 3B 是由该装置执行的数据库检索处理操作的流程图。

假设数据库是在（a）所述的加密处理时加密的并且存储在数据存储设备 316 中。

首先如图 3A 所示的流程图所表示，在数据库检索设定屏幕上输入检索信息（步骤 H11）。输入的检索信息涉及输入要检索的列项，和检索字符串（关键词）。输入信息存储在数据存储设备 316 的检索设定信息存储区 316c。当检索信息通过输入设备 313 输入时，执行预检索处理（步骤 H12）。

如图 3B 所示的流程图所表示在该预检索处理中判定输入检索列项是否预检索处理列项（步骤 I11）。如果是(在步骤 I11 为 yes)，将检索字符串用该列项的公用列密钥加密（步骤 I12）。

预定列项指在加密数据库时设定的要检索的项(用在检索处理中的项），实际上就是对应于‘姓名’，‘州’，和‘年龄’这些项的各项。有关于检索项的信息存储在数据存储设备 316 的加密设定信息存储区 316b。因此，在步骤 I11，通过参考设定在信息存储区 316b 的加密来判定输入的列项是否预定列项。该列项的公用列密钥存储在密钥存储设备 315 中。因此，在步骤 I12，对应于该列项的列密钥从

密钥存储设备 315 读出，并且加密检索字符串。例如，如果指定项是‘州’，将使用例如‘桔子’等加密检索字符串。

如果输入检索列项不是预定列项（不在步骤 I11），将不加密检索字符串。

在上述预检索处理后，检索数据库（参见图 4A）（步骤 H13），作为检索结果获得的数据显示在显示设备 312 上（步骤 H14）。

图 4A 和 4B 说明数据库检索处理。

图 4A 和 4B 是步骤 H13 检索处理实际操作的流程图。

首先，如图 4A 所示的流程图所表示一个检索字符串作为要与数据库比较的字符串在数据存储设备的比较字符串存储区 316d 中设定（步骤 J11）。在此情况下，如上所述，如果输入的检索列项是预定的列项‘姓名’，‘州’，和‘年龄’，那么检索字符串用对应于该列项的列密钥加密，并在预检索处理的比较字符串存储区中设定。如果输入项不是预定的列项就不加密，保持不变，并在比较字符串存储区 316d 中设定。

然后由数据存储设备 316 的数据库存储区 316a 中存储的加密数据库的列编号(column number)确定加密系统（步骤 J12）。于是当要检索的项是用列密钥加密的预定列项时，顺序扫描目标列各行的数据（步骤 J12 和 J13），并将包含在指定行的目标项数据的字符串与在比较字符串存储区 316d 中设定的检索字符串（加密字符串）比较（步骤 J14）。

在比较处理中，如图 4B 流程图所示，从数据库检索的目标项数据的加密字符串与用在检索处理中的加密字符串比较，并且确定他们是否匹配（步骤 K11）。当他们互相匹配时（步骤 K11 为是），包含匹配项的记录数据被提取作为数据库检索结果（步骤 K12）。

该处理重复直到加密数据库终止，相应数据按顺序提取（步骤 J15），提取的数据作为检索结果输出（步骤 J20）。

实际应用中，在图 5（b）示出的加密数据库的举例中，例如，如果在项‘州’，中的佛罗里达等被指定用于检索，接着使用该‘州’的列密钥‘桔子’加密作为检索数据输入的‘佛罗里达’，由此获得‘h*/fDD’。为 h*/fDD 的数据会从‘州’的列中检索出来。于是便可确定对应于‘编号 2’和‘编号 8’的数据存在。

另一方面，当检索项对应于用一个行密钥加密的其他列项之一时，目标列各行数据顺序被扫描（步骤 J12，J16），包含在指定行目标项的数据使用指定给各行的行密钥解密（步骤 J17），然后该结果与在比较字符串存储区 316d 中设定的检索字符串（非加密字符串）比较（步骤 J18）。

在比较处理中如图 4B 流程图所示，判定从数据库检索出的目标列中的数据的解密字符串是否与用在检索处理中的未加密字符串匹配（步骤 K11）。如他们互相匹配，那么将包含匹配项的记录数据提取作为数据库检索结果（步骤 K12）。

该处理重复进行到加密数据库结束。相应的数据顺序提取出来（步骤 J19），并将提取的数据作为检索结果输出。（步骤 J20）。

实际应用中，在图 5(b)所示加密的数据库例子中，例如当项‘体重’中的‘63’数据指定要检索时，‘体重’的行 1 数据使用行密钥例如‘虎’等解密。类似地行 2、3、4、5、6、7、8 和 9 的数据分别使用对应的行密钥 ‘狗’，‘猫’，‘老鼠’，‘象’，‘母牛’，‘兔’和‘狮子’解密，如图 6 所示。然后基于作为检索数据输入的 63，检索‘州’或相应数据列，于是判定对应于‘编号 3’和‘编号 9’的数据存在。

由此，当加密数据库时，用公用列密钥加密检索处理中采用的预定列项。在检索处理中用公用列密钥加密检索数据，并与数据库中加密的数据比较，从而实现了高速检索。另外，列项而不是预定列项相关于各行被赋予不同密钥并且被加密以便提高安全性。在此情况下，

当执行检索处理时，需要使用相关于各行的密钥解密。因此，该检索处理比预定列项的检索处理花费的时间要长，但是这不是一个问题，因为在检索处理中不会频繁使用该项。

根据第一实施例，列项而非预定列项使用相关于各行的特定的行密钥加密。然而根据第二实施例，使用了相关于各行的特定行密钥和一相应列项的公用列密钥在加密处理中组合使用以进一步提高安全性。

图 7 是根据第二实施例的数据库配置示意图；图 7(a)说明加密前状态；图 7(b)说明加密后状态；图 7(c)说明解密后状态。图 8 说明根据第二实施例的组合密钥的配置。

如图 7(a)所示，该装置具有行和列形式的矩阵。此处说明作为一数据库的个人数据。该数据库具有包含以下各项的一记录：‘编号’，‘姓名’，‘体重’，‘身高’，‘年龄’和‘电话’。

数据库使用组合密钥加密。即，当在检索处理中频繁使用的列项包括‘姓名’，‘州’，和‘年龄’时，使用例如‘苹果’，‘桔子’，‘柠檬’等列项中公用列密钥加密列项各行的数据。如图 8 所示，其他的列项‘体重’，‘身高’和‘电话’的各行数据使用列密钥和行密钥的组合密钥例如‘香蕉＋1 个行密钥’，‘荔枝＋1 个行密钥’，‘杏＋1 个行密钥’等加密。

假定‘编号’行不加密。‘虎’，‘狗’，‘猫’，‘老鼠’，‘象’，‘母牛’，‘猪’，‘兔’，‘狮子’用作行密钥。

该些列密钥和行密钥确定一预定非线性函数，加密（解密）处理是用该函数和通过该函数产生的数学向量的二进制运算（逆二进制运算）进行的。在该情况下本发明采用的加密／解密系统将如下所述。

图 7(b)说明使用组合密钥加密图 7(a)所示的数据库的结果。数据存储设备 316 的数据存储区 316a 存储图 7(b)状态数据库。

当检索数据库时，如以上第一实施例所述，检索数据使用对应于

检索时所用列项的公用列密钥加密，然后执行检索处理。例如当要检索项‘州’中的‘佛罗里达’数据时，作为检索数据输入的‘佛罗里达’使用‘州’的列密钥‘桔子’加密，于是获得‘h*/fDD’。为‘h*/fDD’的数据从‘州’列各行检索出来。于是确定对应于‘编号 2’和‘编号 8’的数据存在。

此外，当把加密的数据库恢复为原来状态时，使用加密处理时所用的组合密钥。如图 7(b)所示当使用加密处理数据库所用的组合密钥解密数据时，原来数据能够获得，如图 7(c)所示。

因此加密数据库或检索加密数据库时执行的处理除了列项而不是预定列项的各行数据使用列密钥和行密钥的组合密钥加密外都与上述第一实施例（图 2 到 4B）相同，此处省略对该处理的说明。

于是，检索处理中频繁使用的列项采用列项中公用列密钥加密，由此实现如上述第一实施例所述的高速检索。其他列项使用列密钥和行密钥的组合密钥加密，因而进一步提高安全性。

根据第一和第二实施例，本发明设计为一独立的装置，但也能设计为一个数据库系统，用于通过网络从具有存储在不同位置的数据库的另外信息终端请求一检索处理。

上述所说的数据库系统将描述如下。

图 9 是本发明第三实施例的数据库系统配置的方框图。

该系统包括第一终端设备 320 和第二终端设备 330。第一终端设备 320 通过网络 340 连接到第二终端设备 340。

第一终端设备 320 用作服务器用于提供数据库服务，它包括：一检索设备 321，用于检索一数据库，和一数据存储设备 322，用于存储数据库。第二终端设备 330 用作客户机，请求第一终端设备 320 检索一数据库，并从第一终端设备 320 接收检索结果，第二终端设备包括一检索请求设备 331 和一解密设备 332。

按照该数据库系统，第一终端设备使用以上所述参考图 2 中对应

列项中公用列项加密数据库预定列项各行的数据，使用指定给各行的行密钥加密其他列项各行的数据，并将结果存储在存储设备 322 中。

当第二终端 330 请求第一终端 320 检索一数据库时，第二终端设备 330 如图 3A 所示执行该处理直到预检索处理。即，第二终端设备 330 的检索请求设备 331 判定输入检索列项是否预定的列项，当输入列项是预定列项时使用对应列项中公用列密钥加密一字符串（口令），当输入列项不是预定列项时不请求加密处理。

预检索处理后，第二终端设备 330 通过网络 340 向第一终端设备 320 传送检索字符串。第一终端设备 320 如上所述参考图 4A 和 4B 中通过接收该检索字符串执行该检索处理。

即，第一终端设备 320 的检索设备 321 判定检索列项是否一预定列项，将从第二终端设备 330 获得的检索字符串（加密的字符串）与数据存储设备 322 中加密数据库对应列项的各行数据相比较，如果该列项是预定列项，提取该对应的数据。此外，如果要检索的列项不是预定项，然后数据存储设备 322 中加密数据库对应列项的数据使用各行的密钥解密，从第二终端设备 330 获得的检索字符串（未加密字符串）与各行的解密数据比较，提取对应的数据。

当能够获得检索结果时，第一终端设备 320 通过该网络 340 将与加密数据一样的检索结果返回到第二终端设备 330。第二终端设备 330 与第一终端设备 320 共用一加密密钥。因此当第二终端设备 330 接收来自第一终端设备 320 的检索结果时，解密设备 332 能使用该加密密钥解密该数据。在此情况下，因为加密的数据在第一终端设备 320 和第二终端设备 330 之间传递，故能保证数据库的安全。

因此，即使数据库系统在第一终端设备 320 具有一数据库，通过来自第二终端设备 330 的访问检索数据库，在检索处理中频繁使用的列项数据使用对应列项中公用列密钥加密，而其他列项数据使用指定给各行的行密钥加密，由此提高安全性和实现高速检索。

列项而非预定列项可使用组合密钥加密，该组合密钥包括指定给各行的行密钥和对应列项中公用列密钥，正如前面第二实施例中所描述，因此进一步提高安全性。

根据本发明数据库管理装置的又一实施例将描述如下。

图 10 说明本发明第四实施例的数据库管理装置配置示意图。

该装置加密和管理按行和列矩阵形式设置的数据库。该装置可通过计算机实现以便读出例如存储在磁盘等存储媒体上的程序并且控制计算机的运行。

如图 10 所示，该装置包括 CPU411，一显示设备 412 一输入设备 413，一程序存储设备 414，一密钥产生设备 415，一数据存储设备 416，和一数据 I / F417。

CPU 控制整个装置，读出存储在程序存储设备 414 上的程序并根据该程序执行各种操作。根据该实施例，CPU411 如图 17A 和 17B 所示执行数据库的加密处理和如图 18A 到 19 所示执行数据库的检索处理。

显示设备 412 是一个用于显示数据的设备，例如可以是一 LCD（液晶显示），一 CRT（阴极射线管）等。输入设备 413 是一输入数据的设备，例如可以是一键盘，鼠标等。

程序存储设备 414 包括如 ROM 或 RAM 等；存储该装置必需的程序，该装置需要的程序可以是，数据库加密程序，数据库检索程序等。

程序存储设备 414 可以是除半导体存储器外的磁和光存储媒体。存储媒体包括如便携式媒体 CD－ROM 等和固定媒体如硬盘等。储存在存储媒体上的程序可设计成使部分或全部程序通过如网络电路等的传输媒体从服务器或客户传送到传输控制单元。并且存储媒体可以是网络中提供的服务器的存储媒体，而且程序可以通过如网络电路等传输媒体传输到服务器或客户。

00.10.29

密钥产生设备 415 是用以产生加密数据库使用的加密密钥的设备，在该实施例中它包括：一基本密钥产生单元 415a，一行密钥产生单元 415b，一列密钥产生单元 415c，用于产生三个加密密钥，即分别是基本密钥，行密钥和列密钥。

数据存储设备 416 存储该装置需要的各种数据和表格，它包括 RAM，或例如磁盘设备等的外部存储设备。数据存储设备 416 包括基本密钥参数表 416a，基本密钥存储单元 416b，密钥规范表 416c，加密数据存储单元 416d 和检索字符串存储单元 416e。

基本密钥参数表 416a 是记录基本密钥参数值的表（参见图 13）。基本密钥存储单元 416b 存储操作员按指定操作获得的基本密钥参数值。密钥规范表 416c 是存储相关于数据库（参考图 15）各列（字段）定义的加密系统类型（非加密，行密钥，列密钥）的表。加密数据存储单元 416d 存储加密的数据库。检索字符串存储单元 416e 存储检索数据库时由操作员指定的检索字符串。

数据库 I / F417 是一接口，用于向独立于该装置设置的外部数据库存储设备 418 传送数据和从其接收数据。外部数据库存储设备 418 包含多个数据库文件（原始数据），通过来自该装置的访问指定要选择读出的这些数据库文件。

接着将描述将上述加密系统应用于该装置的数据库的方法。

当加密数据库时，如果将不同密钥用于各行（记录），会给解密密钥造成困难，因而提高了安全性。但是因为加密的数据必须使用相关于各行的密钥解密或当检索数据库时输入的检索数据必须使用相关于各行的密钥加密，如果不同密钥用于每一行，将花费长的时间获得检索结果。另方面，如果数据库使用相关于各行（字段）的不同密钥加密，检索数据只使用对应于要检索的列项的密钥加密,就会以高速检索一数据库。但是当在相同列中存在相同数据时，输出相同加密结果，就可能解密该密钥。

本发明的特点在于：对检索处理中频繁使用的列项数据使用公用密钥（列密钥）加密，对其他列项的数据使用相关于各行的不同密钥（行密钥）加密，而不同于各行的密钥（行密钥）使用行中另外的公用密钥（基本密钥）加密。使用基本密钥的加密处理（解密处理）可确定一预定的非线性函数，并且加密（解密）处理是通过对该函数和用该函数产生的数学向量进行二进制运算（逆运算）执行的。在该情况下的本发明加密／解密系统将在下面描述。

图 20 说明一个实际举例。

图 20 说明本发明该装置数据库的配置； 图 20(a)说明加密前的状态；图 20(b)说明加密后的状态；图 20(c)说明解密后的状态。

如图 20(a)所示，该装置加密按行和列矩阵形式设置的数据库。在该例子中个人数据作为数据库被处理。该数据库包含的各列项（字段）为‘编号’，‘姓名’，‘州’，‘年龄’和‘电话’。

该数据库使用列密钥和行密钥加密。即，当检索处理中频繁采用的列项包括‘州’和‘年龄’时，该列项各行数据（记录）使用列项中公用列密钥加密，而其他列项‘姓名’和‘电话’的各行数据使用相关于各行指定的行密钥加密。这样，该结果存储在记录文件中。此时，当对应列项加密时采用的行密钥使用基本密钥加密，把加密的行密钥加到各记录，并存储该结果。该列项‘编号’不加密。

图 20(b)说明使用列密钥和行密钥加密图 20(a)所示数据库的结果。在此情况下例如‘线密钥’(‘line key’)的列项被加入，并且行密钥（9658，9143，8278，…）加入该列项。图 10 所示的数据存储设备 416 的加密数据存储单元 416(d)在图 20(b)所示状态下存储一数据库。

当检索数据库时，检索数据使用与检索时使用的列项相对应的列密钥加密，然后执行检索处理。例如当检索项‘州’中的‘佛罗里达’数据时，作为检索数据输入的‘佛罗里达’使用‘州’的列密钥加密，

由此得到‘h*/fDD’。为 ‘h*/fDD’的数据从‘州’列各行检索出来。于是确定对应于‘编号 1002’和‘编号 1008’的数据存在出现。

此外当把加密数据库恢复为原来状态时，使用加密处理中采用的列密钥，行密钥和基本密钥。当如图 20(b)所示该数据使用数据库加密处理中采用的列密钥，行密钥和基本密钥解密时，如图 20(c)所示可获得原来数据。

加密／解密数据库的实际配置将描述如下。

图 11 是本发明该装置功能配置方框图。

该装置的输入处理系统包括:基本密钥规范单元 421，基本密钥设定单元 422，密钥规范输入单元 423 和密钥规范设定单元 424。该装置加密处理系统包括：数据读取单元 425，记录输入存储器 426，加密单元 427，加密的记录写入存储器 428，和数据写入单元 429。该装置的加密处理系统包括：加密的记录读出存储器 430，解密单元 431，记录输出存储器 432，和数据输出单元 433。此外，用到上述基本密钥参数表 416a，基本密钥存储单元 416b，密钥规范表 416c 和加密数据存储单元 416d。基本密钥参数表 416a 用于基本密钥设定单元 422。基本密钥存储单元 416b，密钥规范表 416c 和加密数据存储单元 416d 均用于加密单元 427 和解密单元 431。

图 11 所示的各类存储器 426，428，430 和 432 是一寄存器组并设置在数据存储设备 416 的预定区。

当使用该配置加密数据库时，通过基本密钥规范单元 421 按照操作员的操作指定基本密钥。基本密钥设定单元 422 从基本密钥参数表读出由基本密钥规范单元 421 规范的基本密钥参数值，将它在基本密钥存储单元 416b 中设定。

实际上，如图 12 所示通过基本密钥设定对话规范该基本密钥。该基本密钥设定对话是一屏幕，用于由操作员选择基本密钥规范。在屏幕上设置基本密钥规范按钮单元 441，OK 按钮 442，取消按钮 443。

基本密钥规范按钮单元 441 包括多个按钮。当操作员按压这些按钮中的一选择按钮时，基本密钥参数值取决于按压按钮位置。OK 按钮 442 用于确保基本密钥的规范，而取消按钮 443 用于取消该基本按钮的规范。

例如，假定 16 个按钮 1 到 16 从左到右顺序地设置在基本密钥规范按钮单元 441。如图 13 所示基本按钮参数值相应于在基本密钥参数表 416a 上这些按钮的位置被定义。当操作员在基本密钥规范按钮单元 441 上按压按钮 1 时，根据基本密钥参数表 416a 确定基本密钥参数值为 5。类似地，当按压基本密钥规范按钮单元上的按钮 2 时，确定基本密钥参数值为 7。

然后，外部数据库存储设备 418 被访问，要加密的数据库从存储在外部数据库存储设备 418 中各种数据库中指定。指定该数据库后操作员通过密钥规范输入单元 423 为数据库各数据项指定一密钥规范。该密钥规范设定单元 424 通过密钥规范输入单元 423 按照密钥规范指定的操作输入密钥规范表 416c 中的密钥规范信息。

实际上如图 14 所示，密钥规范通过密钥规范设定对话输入。密钥规范设定对话是一屏幕，在其上操作员对数据库各矩阵项（字段）选择地指定加密系统（在加密时使用的密钥类型）。在屏幕上设置有加密系统规范列 451，OK 按钮 452 和一取消按钮 453。

作为一加密系统，每行可用一密钥（行密钥），或可以用各列中的公用密钥（行密钥）。在该例中，一值能输入到加密系统规范列 451 作为用于数据库各列项的加密系统。该值可以是 0（非加密），1（行密钥），或 2（列密钥）。OK 按钮 452 用于设定密钥规范。取消按钮 453 用于取消设定的密钥规范。当加密系统在密钥规范设定对话中指定时，规范内容作为用于各列项的密钥规范信息输入密钥规范表 416c。

图 15 表示密钥规范表 416c 中条目的举例。

在该例中，数据库列编号 1 的项设定为非加密，列编号 2 的项设定为行密钥，列编号 3 的项设定为列密钥，列编号 4 的项设定为列密钥，列编号 5 的项设定为列密钥。具有列编号 1 的项是‘编码’。具有列编号 2 的项是‘姓名’，具有列编号 3 的项是‘州’，具有列编号 4 的项是‘年龄’，列编号为 5 的项是‘电话’。

当基本密钥在基本密钥存储单元 416b 中设定，且当用于各列项的密钥规范信息在密钥规范信息表 416c 中设定时，根据该设定信息数据按下面步骤加密。

即，如图 11 所示由外部数据库存储设备 418 指定的数据库由数据读单元 425 按行单元（记录单元）读出，并顺序地存储在记录输入存储器 426 中。加密单元 427 利用基本密钥参数表 416a 和基本密钥存储单元 416b 加密存储在记录输入存储器 426 中的记录。

参考图 6 将加密处理详细描述如下。

由加密单元 427 加密一记录后，将其存储在加密记录写入存储器 428。通过数据写入单元 429 写入加密数据存储单元 416d。于是在加密数据存储单元 416d 中产生加密数据库。

按照逆步骤解密数据库。

即，首先，将存储在加密数据存储单元 416d 中的加密数据库按行单元（记录单元）读出，顺序地存储在加密记录读出存储器 430。解密单元 431 利用密钥规范表 416c 和基本密钥存储单元 416b 解密存储在加密记录读出存储器 430 中的加密记录。解密处理将参考图 16 详细描述。由解密单元 431 解密的记录存储在记录输出存储器 432，然后通过数据输出单元 433 输出到数据文件 434。于是，在数据文件 434 中产生解密数据库。如图 10 所示数据文件设置在数据存储设备 416 的预定区中。

图 16 说明一实例。

图 16 说明根据本发明的该装置加密和解密数据库时的流程。

假设指定要加密的数据库行 1 的记录由数据读单元 425 读出，并存储在记录输入存储器 426 中。在该情况，利用图 20(a)所示数据库为例，数据含 5 项，即，‘1001’，‘约翰’，‘纽约’，‘22’，‘407－228－6611’，位于数据库行 1 被顺序存储在记录输入存储器 426 中。

加密单元 427 参照密钥规范表 416c 加密相关于各项的 5 项记录。例如图 15 示出了在密钥规范表 416c 中设定的内容，相应于列编号 1 记录的第一项数据（‘编号’）不加密，照原样写到加密记录写存储器 428 中。

此外，相应于列编号 2 记录的第二项数据（‘姓名’）用行密钥加密并写到加密记录写存储器 428。行密钥利用行编号和随机号随机产生，并将不同值用于各行。相应于列编号 3 记录的第三项（‘州’），数据利用列密钥加密。该列密钥具有在列中的公用值。

类似地相应于列编号 4 记录的第 4 项（‘年龄’）数据利用列密钥加密，相应于列编号 5 记录的第 5 项（‘电话’）数据利用行密钥加密。然后将他们写到加密记录写存储器 428。于是，在加密记录写存储器 428 中产生 1 行加密数据为‘1001’，‘wjls’，‘noevjolc’，‘jh’,和‘jgdltytfhDSK’。

进一步，加密单元 427 利用在基本密钥存储单元 416b 设定的参数值和行中公用的基本密钥加密加密记录时用过的行密钥，然后把加密后的行密钥加到加密记录写存储器 428 中。在图 16 的该例中数据‘9658’是加密后的行密钥。

上述处理在数据库各行重复执行，加密的数据库存储在加密数据存储单元 416d 中，图 20(b)示出该状态如下。

当执行解密处理时执行与加密处理相反的处理。

即，把存储在加密数据存储单元 416d 中的加密数据库按记录单元读出到加密记录读出存储器 430。假定行 1 的加密记录读出到加密

记录读存储器 430 中。在上述例中，含有行密钥的 6 项加密数据即‘1001’，‘wjls’，‘noevjolc’，‘jh’，‘jgdltytfhDSK’，和‘9658’顺序存储在加密记录读存储器 430 中。

解密单元 431 参照密钥规范表 416c 相应于各项解密该 6 项数据记录。在图 15 的示例中，相应于列编号 1 的第一项（‘编号’）数据为非加密，该数据照原样写到记录输出存储器 432 中。

相应于列编号 2 的第二项（‘姓名’）数据利用行密钥解密，将其结果写到记录输出存储器 432。因为行密钥在加密处理时是利用基本密钥加密的，该行密钥利用该基本密钥解密以便恢复为原来的数据。此外，相应于列编号 3 的第三项（‘州’）数据利用列密钥解密并写到记录输出存储器 432。

类似地相应于列编号 4 的第四项（‘年龄’）数据利用列密钥解密，相应于列编号 5 的第四项（‘年龄’）数据利用行密钥解密。该些结果均写到记录输出存储器 432。因而在记录输出存储器 432 中产生 1 行解密数据（原始数据），即，‘1001’，‘约翰’，‘22’，‘州’，‘407－228－6611’。

上述处理在加密数据库各行重复执行，并将解密数据库存储在数据文件 434 中，图 20（c）说明了该状态。

根据本发明该装置的操作将参考流程图描述如下。

在该例中，对加密数据库时执行的处理(a)和检索数据库时执行的处理(b)分别进行描述。用于实现流程中各功能的程序是 CPU 可读程序代码储存在程序存储设备 414 的存储媒体中。程序可作为程序代码通过如网络电路的传输媒体可进行传输。

(a) 当加密数据库时：

图 17A 和 17B 是本发明的该装置执行数据库加密处理操作的流程图。假定非加密数据库存储在外部数据库存储设备 418 中。图 17A

示出该状态。

如图 17A（步骤 N11）当加密数据库时，首先设定基本密钥。如上所述基本密钥通过基本密钥设定对话设定。

即，如图 17B 流程图所示，当加密数据库时图 12 所示基本密钥设定对话显示在显示设备 412 上（步骤 O11）。该基本密钥设定对话用基本密钥规范按钮 441 提供，操作员在多个设置在基本密钥规范按钮单元 441 的按钮中按压选择的按钮用以指定一基本密钥。在操作员按压基本密钥规范按钮 441 中选择的按钮后，如果操作员按压 OK 按钮 452 就指定了一个基本密钥（步骤 O12），然后如图 13 所示，从基本密钥参数表 416a 读出相应于该按钮位置的基本密钥参数值，并在基本密钥存储单元 416b 中设定（步骤 O13）。

然后，指定要加密的数据库。根据本发明，与本装置无关的外部数据库存储设备 418 存储各种数据库（原始数据）。因此，当执行加密处理时，外部数据库存储单元 418 通过数据库 I / F417 被访问，要加密的数据库应被指定。

指定要加密的数据库后，设定该数据库检索处理用的列项和设定非加密列项（步骤 N13）。并确定相关于各列项的加密密钥（行密钥和列密钥）（步骤 N14）。

如图 14 所示通过密钥规范设定对话执行设定处理。该密钥规范设定对话是一屏幕，由操作员在其上对于数据库各列（字段）选择地指定一加密系统(用在加密中的密钥类型)。当指定要加密的数据库时该屏幕显示在显示设备 412 上。在该例中，如图 13 所示，可将一作为相关于数据库各列项的加密系统的值输入到密钥规范设定对话的加密系统规范列 451。该值可以是 0（非加密），1（行密钥），或 2（列密钥）。

在该情况下，图 20(a)所示的数据库中，用在检索处理的列项为列 3 是‘州’，列 4 是‘年龄’。并为该些列项指定为列密钥，为其

他的项列 2 的‘姓名’和列 5 的‘电话’指定行密钥。非加密列项是列 1‘编号’。

设定操作后加密数据库操作如下所述。

即，如图 11 所示，该数据库各行数据顺序地从第一行起读到记录输入存储器 426（步骤 N15）。此时由基于由密钥产生设备 415 的行密钥产生单元 415b 赋值各行的行数和随机数随机地产生行密钥，并且将该行密钥存储在数据存储设备 416 的预定区（步骤 N16）。

读到记录输入存储器 426 的行数据的各列项顺序地从第一列起被指定（步骤 N17），并根据存储在密钥规范表 416c 中的密钥规范信息确定相关于指定列项的加密系统（步骤 N18），并利用一个行密钥或 1 个列密钥加密（步骤 N19 到 N22）。

实际上，因为该数据库第一列项‘编号’在图 15 所示密钥规范表 416c 上设定为非加密，不采取行动（步骤 N18，N23）所以项‘编号’保持原数据。

因为相关于第二行中的项‘姓名’设定了 1 行密钥，相应于步骤 N16 产生的该行编号的该行密钥（指定给各行），并从数据存储设备 416 的预定区读出（步骤 N18，N21），然后利用该行密钥加密第二列的数据（步骤 N22）。

此外，因为相关于第三列项‘州’设定了一个列密钥，相应于该列编号的该列密钥（列中公用密钥）通过密钥产生设备 415 的列密钥产生单元 415c 产生（步骤 N18 和 N19），并利用该列密钥加密第三列中数据（步骤 N20）。

类似地，第 4 列的项‘年龄’利用列密钥加密，而第 5 列的项‘电话’利用行密钥加密。

如图 11 所示各列项加密数据存储在加密记录写存储器 428。当加密最后项时，该行密钥利用基本密钥加密，该行密钥是在行数据的第二和第三列进行加密时采用的行密钥。并将其加到密钥记录写存储

器 428（步骤 N25）。该基本密钥由密钥产生设备 415 的基本密钥产生单元 415a 产生。该基本密钥产生单元 415a 从基本密钥存储单元 416b 读出如图 12 所示的基本密钥设定对话，由操作员设定参数值，并产生基于该参数值的一基本密钥。

当通过利用基本密钥加密行密钥获得的 1 行加密数据和数据存储在加密记录写存储器 428 时，该数据存储在加密数据存储单元 416d（步骤 N25）中。

上述加密处理在各行重复执行（步骤 N26 到 N15）。当所有行数据全加密时，加密数据库的最终状态如图 20(b)所示。在该加密数据库中，利用基本密钥加密行密钥，并加到各行的最后项。

(b) 当检索数据库时：

检索加密数据库的处理将描述如下。

图 18A 和 18B 是本装置执行的数据库检索处理操作流程图。假定数据库在上述(a)所示加密处理中被加密，并存储在基本密钥存储单元 416b 中。

首先，如图 18A 的流程图所示，检索信息在图 18A 未示出的数据库检索设定屏幕上输入（步骤 P11）。输入的检索信息指示输入检索列项和检索字符串（关键词）。输入信息存储在数据存储设备 416 的预定区。当检索信息通过输入设备 413 输入时，执行预检索处理（步骤 P12）。

在预检索处理时，如图 18B 所示，判定输入的检索列项是否一预定列项（步骤 Q11）。当判定输入项是预定的列项时（步骤 Q11 为是），用列项中公用列密钥加密检索字符串（步骤 Q12）。

预定列项指示一个在加密数据库时设定的检索项。实际上它指示‘州’和‘年龄’的各项。相关于检索项设定一列项。因此，判定一输入项是否一预定列项，该判定取决于参照密钥规范表 416c 对相应

列项设定的密钥类型。如果输入项是预定列项，然后由密钥产生设备415 的列密钥产生单元 415c 产生相应于该列项的一列密钥，并利用该列密钥加密检索字符串。

如果输入的检索列项不是预定列项（步骤 Q11 为否）,然后如上所述检索字符不加密。

在上述的预检索处理后，检索数据库（参考图 19A 和 19B）（步骤 P13），和作为检索结果获得的数据显示在显示设备 412 上（步骤 P14）。

图 19A 和 19B 是步骤 P13 检索处理实际操作的流程图。

首先，如图 19A 流程图所示，将一检索字符串设定为与数据存储设备 416 的检索字符串存储单元 416e 中的数据库相比较的字符串（步骤 R11）。在该情况下，如果输入项是检索列项(‘州’,‘年龄’)，然后将检索字符串利用相应于预检索处理中列项的列密钥加密和将该结果在检索字符串存储单元 416e 中
设定。如果输入项不是检索列项，则不加密该输入项，并照原样将其设定在检索字符串存储单元 416e 中。

接着，基于该列编号确定存储在数据存储设备 416 的基本密钥参数表 416a 中的加密系统（步骤 R12）。如果检索项是利用一个列密钥加密的预定列项，顺序扫描目标列中各行数据（步骤 R12 和 R13），并将该行的加密字符串与设定在检索字符串存储单元的检索字符串（加密字符串）相比较（步骤 R14）。

在该比较处理中，将从数据库检索的行加密字符串与该加密的检索字符串比较如图 19B 流程图所示，并判定他们是否匹配（步骤 S11）。如果他们互相匹配（在步骤 S11 为是），则将包括匹配项的记录数据提取出来作为数据库检索结果（步骤 S12）。

重复该处理直到加密数据库结束。相应的数据顺序地被提取（步骤 R15），并将提取的数据作为检索结果输出（步骤 R21）。

实际上，在如图 20(b)所示加密数据库的示例中，当指定检索‘州’项中数据‘佛罗里达’时把作为检索数据输入的‘佛罗里达’利用列 3 中‘州’的列密钥加密，由此获得‘h*/fDD’。数据‘h*/fDD’是从‘州’列中检索出的。于是对应于 1001 和 1008 的编号的数据出现。

当检索项是利用行密钥加密的列项时，顺序扫描目标列行数据（步骤 R12，R16）。因为当加密每个行数据时所用的每个行密钥是用基本密钥加密的，所以解密每个行密钥时必须利用基本密钥（步骤 R17）。当利用基本密钥解密各行密钥时，各行加密字符串利用行密钥解密（步骤 R18），并将解密字符串与设定在检索字符串存储区 416e 中的检索字符串（非加密字符串）相比较（步骤 R19）。

在比较处理中，把从数据库检索的该行加密字符串与加密的检索字符串相比较如图 19B 流程图所示，并判定他们是否匹配（步骤 S11）。如果他们互相匹配（在步骤 S11 为是），则将包括该匹配项的记录数据作为数据库检索结果提取出来（步骤 S12）。

重复该处理直到加密数据库结束。顺序提取相应的数据（步骤 R20）。并把提取的数据作为检索结果输出（步骤 R21）。

实际上如图 20(b)加密数据库示例中，当指定检索项‘姓名’中数据‘约翰’时，对应于‘姓名’行 1 的行密钥‘9658’（加密数据）利用基本密钥解密，并且行 1 的‘WJIS’利用行密钥解密，由此获得数据‘约翰’。类似地，对应于各行的行密钥（加密数据）利用基本密钥解密后，通过利用行密钥解密各行数据获得原始数据。如图 20(c)所示，利用各行密钥解密项‘姓名’各行数据后，从解密数据检索出作为与检索数据输入的‘约翰’符合的数据。于是确定对应于‘1001’骗号的数据存在。

因而，当加密数据库时，利用公用列密钥来加密检索处理中所用的预定列项以使检索数据能利用检索处理中的公用列密钥加密，并与

数据库中的加密数据相比较，由此实现了高速的检索处理。

根据该第四实施例，本发明数据库被设计在设备单元，但可通过把终端分为数据库管理的终端和数据库检索终端，将数据库设计在终端单元。

根据本发明的第五实施例的数据库系统将描述如下。

图 21 是根据第五实施例的数据库系统配置方框图。

本系统包括：服务设备 1100 和多个（本例中为 3 个终端）便携终端 1200a，1200b，1200c，…服务设备 1100 与各便携终端 1200a,1200b，1200c,…联机通信，并且他们通过存储媒体 1400a,1400b，1400c,…传递数据。

服务设备 1100 用作服务器用于提供数据库服务，它包括：分布数据收集设备 1101，用于收集分布到各终端的数据；一加密设备 1102，用于加密一数据库，一 AP 软件存储单元 1103，用于存储各种应用软件(AP)；和一数据库存储单元 1104，用于存储各种数据库。AP 软件存储单元 1103 和数据库存储单元 1104 可以是象磁盘设备等的数据存储设备。此外，该服务设备 1100 也可包括通常为通用计算机提供的显示设备和输入设备等。（未在附图中示出）。

另一方面，便携终端 1200a，1200b，1200c，…用作客户机，用于接收来自服务设备的数据库。

便携终端 1200a，包括：解密设备 1201a，用于解密加密的数据库；数据库检索设备 1202a，用于检索数据库。便携终端 1200b 和 1200c 具有类似的配置，并分别包括：解密设备 1201b 和 1201c；数据库检索设备 1202b 和 1202c。向便携终端 1200a，1200b，1200c，…提供媒体读出的设备还有显示设备，输入设备等，虽然他们未在附图中示出。该些便携终端 1200a，1200b，1200c…不具有联机观看数据的浏览功能。但通过存储媒体 1400a,，400b，1400c，…可与服务设备 1100 传递数据。

存储媒体 1400a,1400b，1400c，…是例如含有 CF 卡（致密闪速存储器卡）的存储媒体。卡读写器 1300 是用于向存储媒体 1400a,1400b，1400c，…写入数据和从其读出数据的设备，并且它连到服务设备 1100。

按该配置，服务设备 1100 读出由操作员从数据库存储单元 1104 的各种数据库中指定的数据库，并通过加密设备 1102 加密。在该情况下，加密设备 1102 按照与第四实施例采用的方法相同的方法加密数据库。即，在检索处理中使用的预定列项用公用列密钥加密，同时列项而非预定列项用相关于各行的不同密钥加密，并且行密钥用基本密钥加密。

由加密设备 1102 加密的数据库存储在文件中，而加密的数据文件使用卡读写器 1300 存储在存储媒体 1400a,1400b，1400c，…例如 CF 卡等中。在此情况下，当加密数据文件存储在存储媒体 1400a,1400b，1400c，…时，如图 22 所示，除了加密数据文件 1402，密钥规范表 1403，基本密钥参数表 1404，和应用程序 1401 也均被存储。

密钥规范表 1403 是用于储存相关于数据库各列（字段）限定的加密系统类型（非加密，行密钥，列密钥）的表。并且有类似于第四实施例（参考图 15）密钥规范表 416c 配置的配置。基本密钥参数表 1404 是输入基本密钥参数值的表，并具有与第五实施例基本密钥参数表配置类似的配置（参考图 13）。密钥规范表 1403 和基本密钥参数表 1404 均存储在加密设备 1102 中。应用程序 1401 在数据库检索时使用，并存储在应用软件存储单元 1103 中。

存储媒体 1400a, 1400b，1400c，…分别分布到便携终端 1200a, 1200b，1200c，…，各用户通过把分配的媒体 1400a, 1400b，1400c，…插入她或他自己的终端可检索数据。

即，例如便携终端 1200a 插入分布存储媒体 1400a 并读出存储在

存储媒体 1400a 中的密钥规范表 1403 和基本密钥参数表 1404，还有应用程序 1401 和加密数据文件 1402，用于数据检索处理。然后用于数据检索处理的应用程序 1401 被启动，指定一个预定列项，检索加密的数据文件 1402，并解密和显示作为检索结果获得的数据。

数据检索处理由提供在便携终端 1200a 中的数据库检索设备 1202a 执行。数据库检索设备 1202a 是根据应用程序 1401 操作的。并类似于第四实施例的数据库检索设备。数据通过解密设备 1201a 解密。解密设备 1201a 参照基本密钥参数表 1404 和密钥规范表 1403 执行如第四实施例中的处理的数据库解密处理。

由此，如果数据库系统由与数据库检索终端无关的数据库管理终端设计，因而用户管理的数据库能被加密并存储在存储媒体，并分配给销售的人。由此销售人能利用另外终端检索数据。在此情况下因为存储在存储媒体的数据库是按上述方法加密的，所以数据的安全得到了保证。该存储媒体不仅存储加密数据文件而且存储数据检索应用程序。因此没有必要给便携终端配置数据检索应用程序。该系统用简单便携终端能够实现。

依据该数据库管理装置，列项而不是预定列项数据在执行检索处理时被使用，该列项利用相关于各行的不同密钥被加密；而加密该列项时使用的密钥用另外密钥加密，由此使密钥的解密复杂并实现了高安全性。

用在数据库管理装置中的加密 / 解密系统将描述如下。

图 23 说明加密数据通信系统配置原理，图 23 中 11a,11b 是个人计算机（后面称为 PC），12a，12b 是安全设备。在该例中，数据通信建立在用户 A 的 PC 11a 和用户 B 的 PC 11b 之间。

PC 11a 和 PC 11b 是通用计算机，并且他们分别都连到安全设备 12a 和 12b。安全设备 12a 和 12b 包括 IC 卡。当他们从工厂交付使用时，信息写入了安全设备 12a 和 12b 中。该信息包括 IC 卡生产号，

一组中各成员的用户 ID，和加密密钥（私有密钥 P1，P2），该信息在一组成员中共用，但不公用。

图 24 是 PC 11a 电路和安全设备 12a 配置的方框图。PC 11b 和安全设备 12b 具有与 PC 11a 和安全设备 12a 相同的配置。

PC 11a 是通用计算机包括：CPU21；并通过调用主程序处理数据。存储设备 22，RAM23，键盘 24，显示单元 25 和卡 I / F（接口）26 通过系统总线都连到 CPU21。

存储设备 22 包括：例如硬盘设备，软盘设备，CD－ROM 设备等并存储各种数据、程序等。该例中，它存储要加密的原文数据，后面将描述的鉴别文件等。另外存储在存储媒体（盘等）的程序安装在存储设备 22 中。CPU21 读出安装在存储设备 22 中的程序，并依据该程序执行一处理。

RAM23 用作本发明该装置的主存储器，并存储该装置执行处理时需要的各种数据。键盘 24 是输入设备，用于输入数据和传送各种功能的指令。显示单元 25 例如包括 CRT（阴极射线管），LCD（液晶显示）等，是一个用于显示数据的显示设备。

卡 I / F26 通过连接器 27 连到安全设备 12a，并控制输入数据到安全设备 12a 和从安全设备 12a 输出数据。

安全设备 12a 包括 IC 卡和 CPU31，并通过调用二级程序处理数据。ROM32，RAM33 和闪速存储器 36 通过系统总线连到 CPU31。

ROM32 储存用于实现安全设备 12a 功能的二级程序。RAM33 储存安全设备 12a 执行处理需要的各种数据，该例中它包括：输入缓冲器 34 用于临时存储从 PC 11a 传送的数据，输出缓冲器 35 用于临时存储向 PC 11a 传送的数据。

闪速存储器 36 用作存储设备，用于存储图 25 示出的数据库 41。如图 25 所示，数据库 41 包括成员中共用信息（非公用信息）和指定给各成员的信息（公用信息）。成员中共用信息（非公用信息）包括：

生产号，该组各成员用户 ID，和加密密钥数据（私有密钥 P1，P2）指定给各成员的信息（公用信息）包括加密密钥数据（公用密钥 P3，P4）和口令，口令用作部分公用密钥。

连接器 37 用于电连接安全设备 12a 到 PC 11a，当加密数据通信设置在该系统时，其执行的操作将简述如下（图 23）。

首先，将用作 IC 卡的安全设备 12a 和 12b 传送到一组中各成员。安全设备 12a 和 12b 具有事先输入了生产号，一组每个成员的用户 ID，加密密钥数据（私有密钥 P1、P2）的数据库 41。

各成员将加密密钥（公用密钥 P3、P4）和口令写到安全设备 12a 和 12b。写入的信息存储在数据库 41 公用部分。

当加密数据从 PC 11a 传送到 PC 11b 时，各成员（用户 A 和 B）分别将安全设备 12a 和 12b 插入到 PC 11a 和 PC 11b 以执行加密处理。在此情况下，依据本发明，加密算法依据下面描述的向量的产生。

此时，用于确定产生向量的非线性函数的参数（后面也称为‘常数’）由加密密钥（私有和公用密钥）决定。加密文献和公用密钥一起传送给通信者。在接收侧，利用接收的公用密钥和接收机的私有密钥，用相同的非线性函数产生的向量解密加密文献。

下面描述该实施例的操作。在该实施例中，参照如图 23 所示 PC 11a 和安全设备 12a，该处理操作用以下两种模式分别描述(a)用户条目和(b)数据加密。

(a) 用户条目

首先，当用户利用安全设备 12a 建立加密数据通信时用户形成用户条目。即，赋有安全设备 12a（IC 卡）值的成员把有关图 25 示出的公用部分输入他或她自己的 PC 11a。

图 26(a)和 26(b)是当用户进入完成时 PC 11a 和安全设备执行处理的操作流程图。

用户通过 PC 11a 上的主程序输入用户鉴别数据到 PC 11a。在该情况下，用户鉴别数据指示一用户 ID。主程序把输入的用户 ID 输入给安全设备 12a 的输入缓冲器 34（步骤 A12）。然后它传送控制到安全设备 12a 的二级程序。

在安全设备 12a 侧当程序确认储存在输入缓冲器 34 中的该数据时，读出该数据（步骤 B11）。然后二级程序访问安全设备 12a 的闪速存储器 36，并检查作为用户鉴别数据输入的用户 ID 是否已输入存储在闪速存储器 36 中的数据库 41。其结果是如果用户 ID 还没有输入数据库 41（在步骤 B12 为否），则判定该用户不是该组成员并处理结束（步骤 B13）。

如果用户 ID 已输入数据库 41（在步骤 B12 为是），则判定该用户是该组成员，并请求用户通过 PC 11a 输入他或她的口令和加密密钥（公用密钥）（步骤 14）。

为响应该请求，用户输入他或她的口令和加密密钥（公用密钥）（步骤 A13）。PC 11a 的主程序传送输入的口令和加密密钥（公用密钥）到安全设备 12a 的输入缓冲器 34（步骤 A14）。口令用作公用密钥的一部分。

当从验证为组成员的用户输入口令和加密密钥（公用密钥）时，安全设备 12a 的二级程序读出该输入的信息，需要时将它解密，并把该结果写到储存在闪速存储器 36 中的数据库 41（步骤 B15）。

此时，确定在加密处理中由用户使用的非线性函数。用在该函数中的多个常数由密钥确定。根据本发明的一实施例，多维向量产生函数用作非线性函数，将在下面详细描述。

在处理该信息后，二级程序产生一数据库 41 报表（步骤 B16），将它储存在安全设备 12a 的输出缓冲器 35 中，并向主程序传送控制（步骤 B17）。

当用户验证处理完成时，由主程序使用的加密数据写到上述报

表。在 PC 11a 侧，主程序确认存储在安全设备 12a 的输出缓冲器 35 中的数据，读出该数据，将它作为文件数据写到存储设备 22（步骤 A15）。写入的文件数据作为验证文件，当以后建立加密数据通信时，用于用户的验证检验（步骤 A16）。

（b）数据加密

数据加密实际上涉及加密文献和传送文献。

图 27(a)和 27(b)是当数据加密时由 PC 11a 和安全设备 12a 执行处理的操作流程图，用户使用插入 PC 11a 的安全设备 12a（IC 卡）输入他自己的用户 ID。通过输入的用户 ID 和口令，PC 11a 的用户程序根据验证文件，验证用户（步骤 C12）。

作为验证检验结果（步骤 C121），如果用户不是注册的用户（在步骤 C121 为否），主程序进入终止步骤（步骤 C16）。如果用户是注册的用户（在步骤 C121 为是），主程序传送输入的用户 ID 和口令到安全设备 12a（步骤 C13）。

二级程序在安全设备 12a 上读出用户 ID 和口令（步骤 D11）。然后二级程序把该信息与闪速存储器 36 中数据库 41 的内容相比较，并验证该用户（步骤 D12）。

作为用户验证检验的结果，二级程序产生验证报表用以指示用户是否已经注册到安全系统，将该验证报表传送给安全设备 12a，并将其送到 PC 11a 的主程序（步骤 D13）。

在 PC 11a 侧，主程序读出从安全设备 12a 传送的验证报表，并确认用户已经在安全设备侧验证（步骤 C14）。

如果用户在用户验证检验中遭拒绝，即如果验证报表指示用户不是注册用户（在步骤 C15 为否）；PC 11a 的主程序将它通知给用户，并终止该处理（步骤 C16）。

如果用户在用户验证检验中确认为注册用户，即，如果验证报表

指示该用户是注册用户（在步骤C15为是）。然后PC 11a的主程序执行下面的加密数据通信。

即，主程序从存储设备 22 读出要加密的原文数据（产生的文献），并把它与附加给它的验证报表传送到安全设备12a的输入缓冲器34，然后传送控制到安全设备12a的二级程序（步骤C17）。

验证报表附加到原文数据以使安全设备 12a 确认文献已从安全设备12a验证注册的用户接收。

在安全设备12a侧，二级程序读出从PC 11a传送的原文数据（步骤 D14）。如果没有验证报表加到原文数据（在步骤 D15 为否），则判定该文献未从注册用户收到，由此终止该处理（步骤D16）。

另方面，如果验证报表加到原文数据（在步骤 D15 为是），则判定文献已从注册用户接收，二级程序通过使用多维向量的（后面描述）加密系统加密该原文数据（步骤D17）。然后二级程序存储解密密钥（公用密钥）和加密数据（加密的文献）将其存储到安全设备12a的输出缓冲器35并传送他们到PC 11a（步骤D18）。

PC 11a的主程序接收该解密密钥和该加密的数据（加密的文献）（步骤C18），将它们作为文件输入PC 11a的存储设备22中或传送控制到例如电子邮件的通信软件。并向外部传送他们（到图1示出的PC 11b）（步骤C19）。

下面描述由安全设备12a执行的加密处理的操作。

图28A是加密操作的流程图。

要加密的原文数据（报文数据）定义为M（步骤E11），数据M是二进制数据。安全设备 12a 的二级程序首先将以位单元的加扰（scramble）1应用于该数据M（步骤E12）。得到的数据定义为M′（步骤E13）。

二级程序XORs（得到异或逻辑和）通过把数据M′加到数学上连续产生的随机数，然后执行加密处理（步骤E14）。此时，多维向

量 r 的生成函数用作随机数生成函数，在此情况下，用于生成多维向量 r 的函数，或用于该函数的常数由加密密钥确定（私有和公用密钥）。

即，二级程序当执行加密处理时从数据库 41 读出私有密钥（P1，P2）和公用密钥（P3，P4），依据使用加密密钥作为参数常量的该函数生成多维向量 r 并执行例如 M′ XOR r 的逻辑运算，由此执行加密处理，因而，得到的加密数据定义为 C（步骤 E15）。

实际上如图 29 所示假定 r 是三维向量（x，y，z），向量分量 x，y，z 的计算精度是 16 位。依据后面描述的方程（1），三维向量 r（x，y，z）顺序地产生 r0，r1，r2，r3…。

当已知 M 数据为 m0 m1 m2 m3 m4 m5 m6…的 8 位数据序列(各字符具有 8 位的一字符串），依据计算精度（16 位），M 分解为几个 2 元素（8 位）单元。如果三维向量是 r0，则数据 M 和 r0（x0，y0，z0）进行异或运算（作为异或逻辑和获得），由此进行（x XOR m0 m1）（Y XOR m2 m3）(z XOR m4 m5)的计算，作为计算结果可得到例如 c0 c1 c2 c3 c4 c5…，加密数据 C。

二级程序进一步将加扰（scramble）2 按位单元应用于上述获得的数据 C（步骤 E16）。得出的数据定义为 C′，并将其输出作为最后的加密数据。

在上述处理中，通过重复执行类似用定义 C′ 为 M′ 的加密处理能提高非法解密的难辨程度，如果多维向量 r 生成函数的格式改变，难辨程度还能进一步提高。

通过安全设备 12a 执行的解密处理操作将在下面描述。

图 28B 是解密处理操作的流程图。

解密处理通过执行与加密处理相反的处理能简单地实现。即，假定加密数据定义为 C′（步骤 F11），二级程序首先应用一逆加扰（inverse scramble）2，该逆加扰 2 相反于加密处理时按位单元应用

于数据 C 的加扰 2（步骤 F12）。由此，获得 C 作为应用加扰 2 前的数据（步骤 F13）。

然后二级程序通过例如执行 C XORr 等的计算处理解密数据 C（步骤 F14），由此得到执行加密处理前的数据 M′ 。（步骤 F15）。

该二级程序应用一逆加扰（inverse scramble）1，该逆加扰 1 相反于加密处理时按位单元应用于数据 M′ 的加扰 1（步骤 F12）。因而能获得应用加扰 1 以前的数据，即能获得原文数据 M（步骤 17）。

如果改变生成多维向量的函数的形式重复进行定义 C′ 为 M′ 的 加密处理的过程已加入加密过程，则相应于附加的处理执行解密处理。

依据本发明，一组参数 P（常量）分为两部分，该参数 P 用于在由多维向量 r 执行的加密处理中确定多维向量 r 的函数，该 P 由下式表示。

P＝{Ps，Pp}

其中 Ps 是私有参数，且对应于加密密钥（私有密钥 P1，P2），该加密密钥存储在数据库 41 的非公用部分，而 Pp 是公用参数，且对应于加密密钥（公用密钥 P3，P4），该加密密钥储存在数据库 41 的公用部分。Ps 与 Pp 一起用在验证用户，加密及解密处理中。

依据本实施例，有两个 Ps 和两个 Pp，但很明显参数的数量不局限于本应用中。

依据本发明的一实施例的加密系统将描述如下。

假定在 n(n≥1)维空间的向量是 r，从初始值 r_0 顺序产生新向量 r_j（j＝0，1，2，3，…）的矩阵是 R，此时，向量 r_j 是由下列方程（1）的非线性函数表达的。

$$r_j = a * R(P, r_{j-1})\, r_{j-1} + C \qquad (1)$$

其中 a 是一适当的常系数，P 是用在矩阵中的常数集，并且使用储存在数据库 41 非公用部分的加密密钥（私有密钥 P1，P2）和储存

在数据库 41 公用部分的加密密钥（公用密钥 P3，P4）。C 是用于矢量空间转换的一常向量。

在上述方程（1）中当适当的限定（例如|R|≤1）设置在矩阵时，该系数一集一条件（a sets a conditon）用于多维向量封闭空间区中的各向量。常向量 C 保证向量不收敛到无用点（例如一无意义点具有 r=0）（明显使 c＝0）。

在 n 维空间，向量 r 有 n 个分量（r=x1,x2,…xn），在计算时通常由位长精度表示一数字数据（例如 8 字节或 64 字节）由编译器决定。因此，如果按照连续向量产生方法在一瞬间用 n x m 的数据精度不能再生向量 r，后续向量 r 不能正确地再生（或这样定义矩阵 R）。用向量 r 的初始值 r_0 使向量产生保持正确。即，只有当用 n x m 的位置精度能再生初始值 r_0，后续向量 r_1，r_2，r_3 能保证。

依据本发明实施例的该加密处理，设置了按上述方程（1）获得向量 r 的一个或多个分量，该一或多个分量取决于定义的位长度并且具有相应于总位长的字符串（每个字符串通常是 8 位）在每个位上进行异或运算（异或逻辑处理）这称为第一加密处理，已经在上述参考图 29 的描述中描述。

该步骤作为针对解密的干扰可在双处理中执行。在该情况下上述方程（1）的矩阵 R 能再次改变用以产生新向量使另外的加密处理能按照与第一加密处理相同的方法执行。这个另外的加密处理称为第二加密处理。

在一实例中 n 等于 2（n=2）。首先 R 定义为操作指令其中 r_{j-1} 绕平面上设定的法线旋转 θ 角度，该 R 是 242 矩阵可按下面表达为：

$$R(\theta)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\quad\ldots\ldots(2)$$

在该情况下，θ 是一种参数。即，已知该参数是 r_{j-1} 的函数，并

可按下列方程表达。

$$\theta\ (r) = f(P,\ r) \qquad (3)$$

此时，由上述方程（2）表示的变换能正式由上述方程（1）表示。在该情况下非线性使向量产生过程复杂化。

在上述方程（3）中 P 定义为用在非线性函数 f 中的一组系数并且使用储存在数据库 41 非公用部分的加密密钥（私有密钥 P1，P2）和储存在数据库 41 公用部分的加密密钥（公用密钥 P3，P4）。

由此，在加密处理中通过使用在多维空间顺序产生的向量 r，该加密处理例如与 RSA 的加密处理相比较能够在与计算机精度和特性无关的情况下进行。

此外，容易增加和修改一应用。而且因为本实施例在解密处理中应获得常数 a 常数 P（私有和公用密钥）常向量 c 和向量的初始值 r_0 所有这些数所以使解密处理不能成功进行。

例如，假定 P 含有三维向量的 5 个常数，初始值 r_0 给定的数值由下列方程可知。

1(A)+5(P)+3(r0)+3(C)=12

如果向量中的每个向量是 8 位数字的实数，则全部向量可再生的概率为 10^{-96}。概率几乎等于 0，因此，很难有可能成功解密。

并且在依据本发明的该方法中必须清楚指示确定旋转矩阵 R（θ）的函数 f，由此进一步使非法解密复杂化。

另外，依据上述实施例，使用由限定的私有和公用密钥确定的函数产生一向量，而且使用由限定的至少一个公用密钥确定的函数也能产生一向量。

而且，采用常数时用于确定产生向量的函数的每个常数（a，p，c）是固定的，并且函数也固定。但是，用于确定一函数的常数可如下所述取决于一口令（用作部分公用密钥的加密密钥）。

有可能使用于确定一函数的各常数依赖于加密处理中的一口

令，其中该函数可被确定，以使在 n(n≥1)维空间封闭区中顺序产生的向量彼此不匹配。该口令用作部分公用密钥。该函数应该固定。即，在上述方程（1）中。

a→a(k)

p→p(k)

c→c(k)

其中 a 是一常系数，p 是一组常数（私有密钥和公用密钥）用在矩阵中，c 是用于向量空间变换的一常向量，k 是一口令。

口令 k 由用户输入，存储在数据库 41 的公用部分。二级程序从数据库 41 中读出口令，并依据口令 k 确定上述方程（1）中各常数（a，p，c）。然后，使用基于常数的该函数产生多维向量，并加密数据。

由此通过使确定函数的各常数与口令相关，与固定各常数的情况相比，前者加密的安全性能够改进。

也有可能在加密处理时顺序产生 n(n≥1)维空间封闭区中定义的向量，这样设定一函数使产生的向量不能彼此匹配。用于确定函数的各常数可以取决于口令和实时。口令用作部分公用密钥。该函数是固定的。即，在上述方程（1）中。

a→a(k，t)

p→p(k，t)

c→c(k，t)

其中 a 是一常系数，p 是一组常数（私有和公用密钥），用在矩阵中，c 是用于向量空间变换的常向量，k 是口令，和 t 是一实时。

口令 k 由用户输入并存储在数据库 41 的公用密钥部分。该二级程序从数据库 41 读出口令 k，并基于该口令 k 和实时 t 确定上述方程（1）各常数(a，p，c)。然后使用基于常数的函数产生多维向量和加密数据。

由此，通过使确定一函数的各常数依赖于一口令且使各常数依赖

于实时，各常数不仅依赖于一口令而且还依赖于一实时，由此进一步提高了加密的安全性。

还有可能在加密处理中顺序产生 n(n≥1)维空间封闭区中定义的向量，设定一函数使产生的向量彼此不匹配。用于确定函数的各常数依赖于一口令和一实时相关，另外矩阵函数的选择依赖于一口令。口令用作部分公用密钥。即，在上述方程（1）中。

$a \rightarrow a(k, t)$

$p \rightarrow p(k, t)$

$c \rightarrow c(k, t)$

和

$R \rightarrow R_K$

其中 a 是一常系数，p 是一组常数（私有和公用密钥）被用在矩阵中，c 与一向量同时运动的常向量，k 是口令，和 t 是实时，R 是矩阵。

口令 k 由用户输入，存储在数据库 41 的公用部分。该二级程序从数据库 41 读出口令 k；并基于该口令 k 和实时 t 确定上述方程（1）的各常数(a，p，c)。

二级程序依据口令 k 利用该些常数选择矩阵 R。基于选择的矩阵 R 产生多维向量，并加密数据。

由此，通过使确定函数的各常数依赖于口令，另外使各常数依赖于实时，及通过选择依赖于口令的矩阵，各常数不仅依赖于一口令还依赖于一实时，并且利用该常数的函数也依赖于一口令被选择，由此进一步改进了加密的安全性。

还有可能在加密处理时顺序产生 n(n≥1)维空间闭合区定义的向量，设定一函数以使产生的向量不能彼此匹配。用于确定该函数的各常数可由口令和实时而定。口令用作部分公用密钥。

依据一口令和一实时，选择函数类型。即上述方程（1）中，

a→a(k，t)

p→p(k，t)

c→c(k，t)

和

$R \rightarrow R_K$

其中 a 是一常系数，p 是一组常数（私有和公用密钥）被用在矩阵中，c 是用于向量空间变换的常向量，k 是口令，t 是实时，R 是矩阵。

口令 k 由用户输入，并存储在数据库 41 的公用部分。二级程序从该数据库 41 读出口令，并基于口令 k 和实时 t 确定上述方程（1）各常数(a，p，c)。

二级程序使用与取决于口令 k 和实时 t 的该些常数选择矩阵 R。基于选择的矩阵 R，产生多维向量，并加密数据。

由此，使确定函数的各常数取决于口令，且使之取决于一实时，通过选择取决于口令的矩阵，各常数不仅取决于口令，还取决于实时，利用该常数的函数也依赖于口令和实时选择，由此进一步提高加密安全性。

还有可能在加密处理中顺序产生 n(n≥1)维空间闭合区定义的向量。和通过线性组合多个函数以使产生的向量互相不能匹配，用于确定该函数的一常数可与一口令和实时相关。口令用作部分公用密钥。依据口令和实时选择函数类型。并且，线性组合的系数与口令和实时相关。

假定在一 n(n≥1)维空间内从向量 r 的初始值 r。产生一新向量 r_j(j=0,1,2,3,…)的矩阵是 R_d(d=0,1,2,3,…), 由下列方程可产生新向量。

$$r_j = \sum_d W_d(K,t)\left\{a_d(K,t)R_{d,K,t}(P_j(K,t),r_{j-1}) + c_j\right\}\ldots\ldots(4)$$

上述方程（1）中，a 是常系数, p 是一组常数（私有和公用密钥）被用在矩阵中，c 是用于向量空间变换的常向量，k 是口令，R 是矩阵，和 w 是线性组合系数。

口令 k 由用户输入，并存储在数据库 41 的公用部分。该二级程序从数据库 41 中读出口令 k，和基于口令 k 和实时 t 确定上述方程（4）中的各常数(a，p，c)。通过线性组合多个矩阵二级程序选择一个得出的矩阵 R。

用在矩阵 R 中的线性组合系数 W_d 由口令 k 和实时 t 确定。依据选择的非线性函数（4）产生多维向量来加密数据。

由此使用通过线性组合多个矩阵获得的新矩阵，产生用于确定各矩阵的常数，该常数取决于一口令和一实时，矩阵的选择也依赖于一口令和一实时，线性组合的系数也取决于一口令和一实时，由此提高了加密数据的安全。

此外，在加密处理中，可这样确定该函数，使得在 n(n≥1) 维空间闭合区顺序产生的向量不能互相匹配，由用户选择地定义函数的类型，当把函数应用于主加密算法时可动态地与其他函数组合。

即，相对于顺序产生的多维向量编译的基本加密程序编译用户定义的函数，当执行全部程序时通过动态链接使用编译结果。由此，有预谋的用户例如黑客等几乎能遭到全部拒绝。

如上所述在 n(n≥1) 维空间闭合区定义的向量能顺序地产生，并且通过使用要加密的原文数据和向量分量的逻辑运算产生加密数据。因此，加密处理在没有 RSA 方法需要的精度和特性情况下能够实现。此外，具有高可靠性和易于增加或修改应用的加密处理能够实现。由此，通过把不同的密钥应用于方程 1 中的参数组 p 可定义一个选择的加密数据通信系统。因此仅描述使用公用密钥（私有密钥）的加密 / 解密算法就足够了。下面将详细描述本发明一实施例的加密 / 解密系统。

图 30 说明本发明一实施例的加密／解密系统的原理。

图 30 中在设备 110 和 112 中的安全设备分别位于发送和接收侧，即，加密／解密机存储公用密钥（私有密钥）。当从一设备 110 到另一设备 112 建立加密数据通信时，设备 110 的主程序传送控制到专用硬件安全设备的二级程序。

在发送侧用于执行加密处理的安全设备使用一个随对应于一公用密钥的一参数变化的函数。即，使用一个变换和旋转在 n 维空间闭合区定义的 n 维向量的非线性函数不规则和顺序地产生向量，并且通过在原文数据和产生的向量之间按位单元进行的逻辑运算产生加密数据。

在接收侧用于执行解密处理的安全设备产生与发射侧相同的向量，在产生的向量上执行一相反操作，容易把接收的加密数据解密为原文数据。

在本发明的加密／解密系统中，用于确定非线性函数的参数对第三方是保密的，该非线性函数用于产生上述多维向量。因此，依据本发明，通过至少定义的一公用密钥确定 n 维向量的产生，由此使用非线性函数产生的 n 维向量能够产生混沌以使产生的各 n 维向量不能互相匹配。

即，本发明包括：向量产生单元，用于使用在 n($n \geq 1$) 维空间闭合区定义的各向量分量和角 Ω_n 产生一向量 r_j，该角 Ω_n 由参数组 p 以这样的方法确定，使利用包含至少用于该向量旋转的 n 维旋转矩阵 $R_n(\Omega_n)$(相应于方程 1 中的 R)的非线性函数（相应于方程（1））顺序产生的各向量相关于向量旋转在 n 维空间不能匹配；在加密处理中，一二进制运算单元，用于使用对原文数据和由向量产生单元产生的向量分量进行的一二进制运算产生加密数据；在解密处理中，一逆二进制运算单元，用于在逆二进制运算中产生原文数据，该二进制逆运算对应于使用向量产生单元产生的向量 r_j 和加密数据进行的二进制运

算的相反的运算。

特别是，本发明包括：一旋转矩阵产生单元，用于使用在 n(n≥1)维空间闭合区定义的一向量的分量和由参数组 p 确定角 Ω_n 来产生 n 维旋转矩阵 $R_n(\Omega_n)$ 该 n 维旋转矩阵用该(n-1)维旋转矩阵 $R_{n-1}(\Omega_{n-1})$作为(n-1)维小矩阵来旋转该向量；一向量产生单元，用于产生向量 r_j，使包含至少该旋转矩阵 $R_n(\Omega_n)$的非线性函数顺序产生的各向量 r_j（j≥0)在 n 维空间互相不能匹配；一个二进制运算单元，用于利用原文数据和由向量产生单元产生的向量分量的二进制运算产生加密数据。

本发明的加密／解密系统与当数据发送机和数据接收机使用通用安全设备（加密设备）建立数据通信时执行的加密／处理有关。

依据本加密系统，数据发送机（加密侧）基于预定公用密钥，通过使用已产生原文数据报文的密钥序列按位单元执行预定逻辑运算（通常是异或逻辑和运算）产生密文。数据接收机（解密侧）基于预定公用密钥，通过使用与加密侧相同的密钥序列按位单元执行预定逻辑运算（与加密侧相同的操作）获得原始的原文。

在该加密系统中，多维向量产生设备用作随机数产生设备以产生上述的密钥序列。在该情况下，用于确定多维向量产生设备向量产生函数的不同参数和初始状态作为公用密钥提供。

图 30 说明应用本发明的加密系统的配置举例。加密设备 110 包括：多维向量产生函数单元 101 和逻辑操作处理函数单元 102。

类似地，该解密设备包括：多维向量产生函数单元 121 和逻辑运算操作函数单元 122。

图 30 位于加密侧的加密设备 110 和位于解密侧的解密设备 112 之间，例如使用 IC 卡来分配一公用密钥。在保密状态，共享该公用密钥，位于加密侧的加密设备 110 基于由预定公用密钥确定的函数产生多维向量，使用原文和作为随机数序列的向量分量数据获得异或逻

辑和，以便将原文报文变换为密文并将该密文发送到该解密设备112。

接收到密文的解密设备112通过逻辑运算处理函数单元122从密文产生一向量，该逻辑运算处理函数单元 122 具有与加密设备 110 的多维向量产生函数单元101相同的函数；获得该向量和产生的随机数序列的异或逻辑；及恢复该原始的原文报文。

此外，由于加密设备110和解密设备112执行的处理实际上彼此相同，处理设备，例如计算机等，具有解密设备112和加密设备110二者的功能。

图31说明加密设备110和解密设备112中的解密和加密程序的配置。

主程序131管理输入和输出数据，确定数据是否加密或解密并管理整个加密解密处理。参数表生成库储存用IC卡分配的公用密钥。加密／解密机133从参数表生成库132接收作为参数的公用密钥，基于由多维向量旋转函数生成库134确定的矩阵产生旋转向量，利用向量分量加密原文或解密密文。

下面将详细描述多维向量的产生。

就相关于在多维空间(n维空间)定义的向量r_{j-1}的旋转而论，一般旋转角用Ω_n表示，相应于该旋转的操作用$R_n(\Omega_n)$来表示为一 n x n 矩阵。即$R_n(\Omega_n)$作用于r_{j-1}，并旋转该向量方程，于是（1）可改写为下列方程（5）即，旋转向量的一般方程由此定义了一新的向量r_j。

$$r_j = \alpha R_n(\Omega_n) r_{j-1} + c \qquad (5)$$

其中a是一常数满足$|a| \leqslant 1$，c是n维常向量。上述方程表示新向量r_j是从r_{j-1}通过旋转和空间平移产生。

依据本发明，非线性序列能够这样产生，使产生的r向量序列可以不是混沌的，即，通过设置的旋转角Ω_n在闭合空间中的原始序列取决于r，即，Ω_n可用参数p和向量r的函数正式表示如下列方程(6)

所示（相应于方程（3））。

$$\Omega_n = \Omega_n(P, r_{j-1}) \cdots\cdots (6)$$

其中 p 指示一组用在 Ω_n 的函数中的任意个参数。

$$P=\{P_i \mid i = 1,2,3,\ldots\} \cdots\cdots (7)$$

例如在二维向量中，二维旋转解 Ω_n 用二维向量 r=（x,y)的分量 x 和 y 表示如下式：

$\Omega_2 = p_1x+p_2y+p_3$

其中参数 p_1，p_2 和 p_3 选择地给出。

参考图 32 示出的流程图描述图 30 系统中由加密设备 110 和 112 处理上述二维向量时执行的实际操作。

利用正交坐标系统的分量 x 和 y 由 r=(x,y)表示二维向量 r。相关于向量的角 $\Omega_n = \theta$ 的旋转运行由二维矩阵表示如下。

$$R_2(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \cdots\cdots (8)$$

假定用于旋转向量的函数使用一函数 $\theta = p_1x+p_2y+p_3$ 和获得的旋转角存储在多维向量旋转函数产生库 134（见图 13），和 r_0 的初始值 x_0,y_0 以及 p 值，即，$p_1=1$，$p_2=1$，$p_3=1$ 事先存储在参数表产生库 132（见图 31）作为公用密钥。参考图 32 描述一举例。

为了产生二维向量，初始值 r_0 (包括分量数据 x_0,y_0)和用于定义旋转角 θ 函数的参数 p_1，p_2，p_3 从参数表产生库 132（见图 31）读出并存储在设备（110，112）存储器工作区（步骤 21）。基于 r_0 的值 x_0,y_0 计算 $\theta = p_1*x_{j-1}+p_2*y_{1-1}+p_3$（$\theta = p_1* x_0*p_2*y_0+p_3$）。

然后为了确定旋转矩阵 R 元素值，获得 cos θ 和 sin θ 并作为 cos__t 和 sin_t 分别存储（步骤 23）。

接着由方程 $r_j=aR_2(\Omega_2)r_{j-1}+c$ 计算新向量 r_j（步骤 24），即，执行下列计算，以产生新向量 r_j（分量 x_j, y_j）。

x_j＝a*(“cos_t” *x_{j-1}- “sin_t” *y_{j-1})+c_x;

y_j＝a*(“sin_t” *x_{j-1}+ “cos_t” *y_{j-1})+c_x;

然后，基于向量 y_j 的分量获得连续旋转角 θ （步骤 22）以及重复上述步骤 23 和 24，由此顺序地产生向量。

依据本发明的加密／解密系统，因为对旋转引入三角函数，使用三角函数的乘积，非线性比通常的无规则函数有更多改进，由此使解密更复杂化。

下面描述通过产生多维向量的加密数据处理。

如图 33 所示 n 维旋转矩阵 $R_n(\Omega_n)$在加密处理中首先产生（步骤 41）。产生矩阵的方法下面将详细描述。

使用包含 n 维旋转矩阵 $R_n(\Omega_n)$的非线性函数产生向量（步骤 42）。向量 y_j 顺序产生以使他们在 n 维空间互相不匹配。利用原文数据和由向量产生单元产生的向量分量执行二进制运算，由此产生加密数据（步骤 43）。然后加密数据传输到接收机的接收设备（步骤 44）。

下面描述步骤 43 的二进制运算。

假定每个顺序产生的向量 r 用 N 位表示。例如当二维向量用分量 x 和 y 表示时,每个 x 和 y 的数据值用 16 位表示。x 和 y 的数据按 N 位设置（例如 32 位）。

向量串 $r_j(j=1,2,3,\cdots)$在该步骤获得和通过分割加密原文数据 M 的数据串 $M_j=(j=1,2,3,\cdots)$按 N 位单元表示将 r_j 和 M_j 用作二进制操作数以便获得异或逻辑和（XOR），和结果 $C_j(j=1,2,3,\cdots)$作为加密数据获得。即，进行下列计算。

$$C_j=r_j \text{ op } M_j \qquad (9)$$

上述二进制运算符 op 通常是相关于每个的异或逻辑和(exclusive logical sum)但由于异或逻辑和是可逆的，不适合将其作为加密运算符

使用，为了补偿异或逻辑和的这一缺陷，提出一种加扰 M_j 位的异或逻辑和运算作为二进制运算符,在该情况下出现下列方程。

$$op=XOR*S \qquad (10)$$

其中 S 指示一加扰（scrambling）运算用于加扰 M_j 位，而 XOR 指示作为接着的异或逻辑和运算的定义。然后加密数据由 $C_j=r_j\ op\ M_j$ 获得。

解密处理参考图 33 描述如下

在解密处理中，如象加密处理，首先产生 Ω_n 维闭合区定义的旋转向量的旋转矩阵 $R_n(\Omega_n)$（步骤 45）。向量 r_j 以这种方式顺序产生，即，使由包含旋转矩阵 $R_n(\Omega_n)$的非线性函数产生的各向量在 n 维空间互相匹配（步骤 46）。

然后，解密数据通过使用收到的加密数据与在向量产生步骤 46 产生的向量 r_j 执行逆二进制运算产生相应于步 43 执行的二进制运算的相反运算(步骤 47 和 48）。

在解密处理中连续检索接收的加密字符串 C_j=j=1,2,3,…）以执行一解密运算同时产生相应于 C_j 的向量，该处理用参考图 34 的流程图进行说明。

解密处理由 j=0 开始（步骤 51）在步骤 52 检索加密数据 C_j，在步骤 53 产生 n 维旋转矩阵 $R_n(\Omega_n)$和在步骤 54 产生向量 r_j。然后在步骤 55 执行 $M_j=r_j\ op^{-1}\ C_j$ 的运算以产生解密数据（原文 M_j）如果加密数据还没有完全处理，那么用 j=j+1 接着检索下面的加密数据（步骤 56 和 57）以产生 $R_n(\Omega_n)$，和重复产生连续向量 r_j 的处理。执行重复步骤 52 到 56 的处理直到加密数据全部处理。

此外，上述第一加密和解密实施例可以推广到更实际的加密数据的步骤，第二实施例将在下面描述。

首先，执行下列方程。

$$C_0=r_0\ op\ M_0 \qquad (11)$$

然后计算相关于 C_0 的检验和 Σ_0。并且上述方程（9）可相关于 j 其中 j≥1 改写为下列方程。

$$C_j=(r_j \text{ op } \Sigma_{j-1}) \text{ op } M_j \qquad (12)$$

检验和例如用包含在计算的 C 值内的 IS 数表示如同二进制表示的位数，该位数与 r_j 位数相同。在该方程中，Σ_0 从加密数据 C_0 的值中获得，Σ_1 从 C_1 中获得和 Σ_2 从 C_2 中获得，按以下计算次序。

原文	M_0	M_1	M_2	M_3	…
（密钥串）	r_0	r_1	r_2	r_3	…
密文	C_0	C_1	C_2	C_3	…
	Σ_0	Σ_1	Σ_2	Σ_3	…

即，相关于 M_0 的加密数据 C_0 通过 $C_0=r_0 \text{ op } M_0$ 发射机获得 C_0 因而获得 C_0 的检验和 Σ_0。相关于 M_1 的加密数据 C_1 是由 $C_1=(r_1 \text{ op } \Sigma_0) \text{ op } M_1$ 计算于是获得 C_1 的检验和 Σ_1。连续的数据 M_j 用计及前面数据获得的 Σ_{j-1} 通过 $C_j=(r_j \text{ op } \Sigma_{j-1}) \text{ op } M_1$ 加密。r_j 和 Σ_{j-1} 用相同数据宽度（位数）计算。

用于解密的接收机接收 C_0，C_1，C_2，…，和计算 $M_0=r_0 \text{ op}^{-1} C_0$，并且必须从接收的 C_0 中获得检验和 Σ_0。以此类推 M_1 相关于 C_1 从下式计算。

$$M_1=(r_1 \text{ op } \Sigma_0) \text{ op}^{-1} C_1 \qquad (13)$$

连续数据 M_j 利用相关于接收的 C_{j-1} 通过下列方程解密。

$$M_j=(r_j \text{ op } \Sigma_{J-1}) \text{ op}^{-1} C_j \qquad (14)$$

上述步骤获得的加密数据已经用不同密钥处理，假定针对使用假设密钥解密该数据的企图该数据是永久的。

如果在多维空间旋转系统中维数变大，旋转矩阵元素数变大，于是产生问题即，在加密／解密处理中的运算负担加大。为解决该问题，在加密系统中计算多维空间旋转矩阵的方法使用了具有小维数的伪空间旋转矩阵的多维空间旋转系统。

下面将说明相关于多维空间旋转导出的旋转矩阵 $R_n(\Omega_n)$。

第一种方法是从(n-1)维旋转矩阵 $R_{n-1}(\Omega_{n-1})$中产生 n 维旋转矩阵 $R_n(\Omega_n)$。因为相关于多维空间旋转的方法计算复杂，例如采用两维空间旋转进行的说明描述如下。两维空间向量 r 用正交坐标系统的分量 x 和 y 由下列方程表示。

r=(x, y)

相关于向量的角 $\Omega_n=\theta$ 的旋转运行用两维矩阵表示为

$$R_2(\theta)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\text{.....(16)}$$

其中左侧下标 2 表示在两维空间定义的运算。该运算满足下列方程的条件。

$$|R_2(\theta)|=1\text{.....(17)}$$

$$R_2(-\theta)=R_2(\theta)^{-1}\text{.....(18)}$$

方程（17）保证在旋转运行中旋转向量大小保持不变，而方程（18）表示存在一个旋转运行使旋转向量恢复为原始状态。

推广到三维空间，方程（16）右侧的描述简化并正式由下列表示

$$R_2(\theta)=\begin{pmatrix}\alpha_{11} & \alpha_{12}\\ \alpha_{21} & \alpha_{22}\end{pmatrix}\text{.....(19)}$$

其中 $\alpha_{11}=\alpha_{22}=\cos\theta$ 和 $\alpha_{21}=-\alpha_{12}=\sin\theta$。在三维旋转情况下，使用三个正交轴中的每个作为旋转轴开始旋转是合理的，可以采用下列三个矩阵中任一个表示。

$$R_{3.1}(\theta)=\begin{pmatrix}1 & 0 & 0\\ 0 & \alpha_{11} & \alpha_{12}\\ 0 & \alpha_{21} & \alpha_{22}\end{pmatrix}\text{.....(20-1)}$$

$$R_{3,2}(\theta) = \begin{pmatrix} \alpha_{11} & 0 & \alpha_{12} \\ 0 & 1 & 0 \\ \alpha_{21} & 0 & \alpha_{22} \end{pmatrix} \quad \text{.....(20—2)}$$

$$R_{3,3}(\theta) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & 0 \\ \alpha_{21} & \alpha_{22} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{.....(20—3)}$$

注意他们能通过加 1 获得该 1 作为方程（19）的两维空间旋转运行的对角元素。此外，很明显，运行中三维向量的旋转在图 37A 到 37C 中表示。

上述矩阵（20—1），（20—2），（20—3），是三维矩阵包括了表示二维空间旋转运行的二维矩阵。通过从上述矩阵中检索三个矩阵（矩阵能复制）和连续把矩阵彼此相乘能获得广义的三维旋转。在三维空间广义的旋转角能用下列方程表示。

$\Omega_3 = (\theta_1, \theta_2, \theta_3)$

其中相关于三维向量的旋转运行 $R_3(\Omega_3)$由下列方程表示。

$R_3(\Omega_3) = R_{3,i}(\theta_i)\, R_{3,j}(\theta_j) R_{3,k}(\theta_k)$ .....(21)

其中 i，j 和 k 可以是 1，2 和 3 中任一个。并且在相同轴上不继续运行的条件基础上通常能重复。i，j，k 例如可以是 1，2 和 3。

如果‘逆旋转角’用$-\Omega_3 = (-\theta_1, -\theta_2, -\theta_3)$表示，那么由（21）表示的旋转运行的逆旋转运行用计及有效的下列方程表示。

$$R_3(-\Omega_3) = R_{3,K}(-\theta_k) R_{3,j}(-\theta_j) R_{3,i}(-\theta_i) \quad \text{.....(22)}$$

由方程（21）定义的旋转运行通常得到下列形式

$$R_3(\Omega_3) = \begin{pmatrix} \beta_{11} & \beta_{12} & \beta_{13} \\ \beta_{21} & \beta_{22} & \beta_{23} \\ \beta_{31} & \beta_{32} & \beta_{33} \end{pmatrix} \quad \text{.....(23)}$$

其中矩阵元素从方程（16），（19），（20－1），到（20－3）和（21）中唯一地确定。

相关于 $R_3(\Omega_3)$，满足下列条件。

$$|R_3(\Omega_3)|=1 \quad \text{.....(24)}$$

$$R_3(-\Omega_3) = R_3(\Omega_3)^{-1} \quad \text{.....(25)}$$

在实际的三维空间中向量的产生如下所述。

在三维空间中，向量 r_j 能够由存储的旋转矩阵相乘的排序产生。如果旋转角由 $x_{j-1}=x$，$y_{j-1}=y$，$z_{j-1}=z$ 表示相关于简化说明的三维旋转出现下列方程。

$$\theta_1 = p_{11}x + p_{12}y + p_{13}z + p_{14}$$
$$\theta_2 = p_{21}x + p_{22}y + p_{23}z + p_{24}$$
$$\theta_3 = p_{31}x + p_{32}y + p_{33}z + p_{34}$$

三维空间旋转运行 $R_3(\Omega_3)$如方程（21）所示由下面三个旋转矩阵的相乘表示即：

$$R_3(\Omega_3) = R_{3,i}(\theta_i)\ R_{3,j}(\theta_j)\ R_{3,k}(\theta_k)$$

其中整数 i, j 和 k 是 1，2 和 3 中任一个和通常能重复即，有 $R_{3,1}(\theta_1)$，$R_{3,2}(\theta_2)$，$R_{3,3}(\theta_3)$相乘的，3×2×2（＝12）种方法取决于发射机的参数。在该加密处理中，向量 r_j 在三维空间的产生过程如图 35 所示。

即，$R_3(\Omega_3)$可基于发送机参数指定的乘法排序制备。计算旋转向量角 θ_1，θ_2，θ_3 的函数的初始向量值 r_0 及参数 p_{11} 到 p_{34} 都被存储起来（步骤 62）。然后，用 $r_0(r_{j-1})$的分量（x, y, z）执行以下操作（步骤 63）。

$$\theta_1 = p_{11}x + p_{12}y + p_{13}z + p_{14}$$
$$\theta_2 = p_{21}x + p_{22}y + p_{23}z + p_{24}$$
$$\theta_3 = p_{31}x + p_{32}y + p_{33}z + p_{34}$$

然后计算 $R_3(\Omega_3)$，并由式（5）产生一新向量 r_j。与此同时，由上所述发送机的参数确定乘法的排序。例如，如发送机的职员数等。对于旋转矩阵 $R_3(\Omega_3)$，发送机）接收机不根据发送数据时指定的排序来计算它，但是事先 12 个存储函数，任何一函数均可指定。

以下描述将上述所述二维旋转扩展到三维，从三维扩展到四维的应用过程。

在该情况下，四个二维矩阵，即，$R_{4,i}$ (Ω_3)(i=1,2,3,4),通过把 1 加入方程（23）该 1 作为对角元素，即获得下列方程。

$$R_{4,1}(\Omega_3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \beta_{11} & \beta_{12} & \beta_{13} \\ 0 & \beta_{21} & \beta_{22} & \beta_{23} \\ 0 & \beta_{31} & \beta_{32} & \beta_{33} \end{pmatrix} \quad \text{.....(26—1)}$$

$$R_{4,2}(\Omega_3) = \begin{pmatrix} \beta_{11} & 0 & \beta_{12} & \beta_{13} \\ 0 & 1 & 0 & 0 \\ \beta_{21} & 0 & \beta_{22} & \beta_{23} \\ \beta_{31} & 0 & \beta_{32} & \beta_{33} \end{pmatrix} \quad \text{.....(26—2)}$$

$$R_{4,3}(\Omega_3) = \begin{pmatrix} \beta_{11} & \beta_{12} & 0 & \beta_{13} \\ \beta_{21} & \beta_{22} & 0 & \beta_{23} \\ 0 & 0 & 1 & 0 \\ \beta_{31} & \beta_{32} & 0 & \beta_{33} \end{pmatrix} \quad \text{.....(26—3)}$$

$$R_{4,4}(\Omega_3) = \begin{pmatrix} \beta_{11} & \beta_{12} & \beta_{13} & 0 \\ \beta_{21} & \beta_{22} & \beta_{23} & 0 \\ \beta_{31} & \beta_{32} & \beta_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{.....(26—4)}$$

进而在四维空间旋转角 Ω_4 的旋转运行由下式定义：

$$R4(\Omega 4)=R4,i(\Omega 3,i)R4,j(\Omega 3,j)R4,k(\Omega 3,k)R4,l(\Omega 3,l)\ldots\ldots(27)$$

$\Omega_{3,i}$=(i=1,2,3,4)是另外的三维旋转角 Ω_3，不同于上述定义的角。

通过重复进行定义，在 n 维空间相关于角 Ω_n 的旋转操作通常由下式表示

$$R_n(\Omega_n)=\prod_{i=1}^{n}R_{n,j}(\Omega_{n-1,i})\ldots\ldots(28)$$

容易确认获得的旋转运行满足方程（29）和（30）的特征通过估计方程（28）右侧乘积的排序。

$$|R_n(\Omega_n)|=1\ldots\ldots(29)$$
$$R_n(-\Omega_n)=R_n(\Omega_n{}^{-1})\ldots\ldots(30)$$

n 维旋转矩阵 $R_n(\Omega_n)$通过执行图 36 流程的处理能够产生。

即，首先设置 k＝2(步骤 30)，产生 2 维旋转矩阵 $R_2(\Omega_2)$（步骤 31）。然后判断 k 值是否小于 n（步骤 32）。如果是，k 值增 1(步骤 33)，产生 k 维旋转矩阵 $R_k(\Omega_k)$以使它能包括（k-1）维旋转矩阵 $R_{k-1}(\Omega_{k-1})$作为（k-1）维小矩阵（步骤 34）。

于是，k 产生的 k 维旋转矩阵 $R_{kj1}(\theta_{j1})$, $R_{kj2}(\theta_{j2})$,…，$R_{kjk}(\theta_{jk})$的乘积获得,从而获得旋转矩阵 $R_k(\Omega_k)$（步骤 35）。然后从 k=2 到 k=n 重复步骤 34 和步骤 35，能产生 n 维旋转矩阵 $R_n(\Omega_n)$。

在下面说明的第二种方法中，通过设置多个小维数旋转矩阵作为对角块能获得伪旋转矩阵。该小维数旋转矩阵具有设置为 0 的保留元素（remaining element）。第二种方法将详细说明如下。在六维空间的旋转矩阵 R 的元素由下列方程（37）表示显示了大量计算。

$$R=\begin{pmatrix} R_{1,1} & R_{1,2} & R_{1,3} & R_{1,4} & R_{1,5} & R_{1,6} \\ R_{2,1} & R_{2,2} & R_{2,3} & R_{2,4} & R_{2,5} & R_{2,6} \\ R_{3,1} & R_{3,2} & R_{3,3} & R_{3,4} & R_{3,5} & R_{3,6} \\ R_{4,1} & R_{4,2} & R_{4,3} & R_{4,4} & R_{4,5} & R_{4,6} \\ R_{5,1} & R_{5,2} & R_{5,3} & R_{5,4} & R_{5,5} & R_{5,6} \\ R_{6,1} & R_{6,2} & R_{6,3} & R_{6,4} & R_{6,5} & R_{6,6} \end{pmatrix} \quad \text{.....(37)}$$

另外，旋转矩阵 R 用伪旋转矩阵代替它计算。伪旋转矩阵 Q 由设置多个小维数空间旋转矩阵作为对角块获得，该小维数空间旋转矩阵具有设置为 0 的保留元素。例如在六维空间伪旋转矩阵 Q 用方程（38）表示。

$$Q=\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}=\begin{pmatrix} A_{1,1} & A_{1,2} & A_{1,3} & 0 & 0 & 0 \\ A_{2,1} & A_{2,2} & A_{2,3} & 0 & 0 & 0 \\ A_{3,1} & A_{3,2} & A_{3,3} & 0 & 0 & 0 \\ 0 & 0 & 0 & B_{1,1} & B_{1,2} & B_{1,3} \\ 0 & 0 & 0 & B_{2,1} & B_{2,2} & B_{2,3} \\ 0 & 0 & 0 & B_{3,1} & B_{2,3} & B_{3,3} \end{pmatrix} \quad \text{.....(38)}$$

其中 A 和 B 是三维旋转矩阵。

当伪旋转矩阵 Q 的元素与旋转矩阵 R 的元素比较时，Q 包含较多的零元素。由此需要少量计算。它的加密函数有效操作。通常多维空间旋转矩阵 Q 能设置为下列方程（39）表示。

$$Q=\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & A_i \end{pmatrix} \quad \text{.....(39)}$$

其中 A_1，A_2，$\cdots A_i$ 是多维空间旋转矩阵

由此计算量可显著减少，通过用伪旋转矩阵置换多维空间旋转系统的旋转矩阵可快速执行加密和解密处理。该伪旋转矩阵是通过设置

多个作为对角块（diagonal blocks）（具有设置为 0 的保留元素）的小维数旋转矩阵获得。

在又一方法中，把在通过下列方程（40）表示的小变换中获得的 P 值用作一伪空间旋转矩阵。

$$P=S*Q*S^{T} \qquad (40)$$

在方程（40）中，q 是上述伪矩阵，而 s 是置换矩阵。如下列方程（41）所示，它是具有各行和列并包含 1 作为元素的方程。

$$S=\begin{pmatrix}0&0&1&0\\0&1&0&0\\0&0&0&1\\1&0&0&0\end{pmatrix}\qquad\ldots\ldots(41)$$

例如当伪旋转矩阵 Q 用上述（六维空间）方程（38）表示时，伪空间旋转矩阵 p 用下列方程（42）表示。

$$P=\begin{pmatrix}A_{1,1}&0&A_{1,2}&0&A_{1,3}&0\\0&B_{1,1}&0&B_{1,2}&0&B_{1,3}\\A_{2,1}&0&A_{2,2}&0&A_{2,3}&0\\0&B_{2,1}&0&B_{2,2}&0&B_{2,3}\\A_{3,1}&0&A_{3,2}&0&A_{3,3}&0\\0&B_{3,1}&0&B_{3,2}&0&B_{3,3}\end{pmatrix}\qquad\ldots\ldots(42)$$

一实例由下列方程（43）表示

$$S=\begin{pmatrix}1&0&0&0&0&0\\0&0&0&1&0&0\\0&1&0&0&0&0\\0&0&0&0&1&0\\0&0&1&0&0&0\\0&0&0&0&0&1\end{pmatrix}\qquad\ldots\ldots(43)$$

由此，通过用组合的置换矩阵（permutation matrice）获得的伪旋转矩阵代替多维空间旋转系统的旋转矩阵使计算处理复杂化，于是进一步增加了解密的难度。该置换矩阵具有多个设置为零的保留元素

的作为对角块设置的小维素旋转矩阵。

本加密系统的特征是用增加空间维数增加解密加密数据的难度，但软件处理能快速进行。由此不需要特殊硬件进行加密和解密处理，能精确指示分级特许（授权）和用于个人，用于组等的解密。

因此，本发明的应用包括：个人或私有数据的管理，保密邮件的管理、广播通讯数据等的管理，和各种其他领域。此外因为本发明能增强因特网环境服务器中数据的安全，所以系统管理人员和因特网服务的提供者可充分利用本发明。

此外，依据本发明参数 p 和常向量 c 可依赖于时间，并且 p 能由下列方程表示。

$$P(t)=\{p_i(t):i=1,2,3,\cdots\cdots\} \qquad (31)$$

其中 c 可设置为 c(t)。另外向量初始值 r_0 也能依赖于 t。

在实际加密处理中，向量初始值 r_0 代替右侧的 $r_{j-1}(j=1)$。获得的新向量 r_1 代替了方程（5）右侧的 r_{j-1}。通过重复该处理，顺序产生新向量。由方程（31）表示的时间依赖关系表示相同的加密数据不能获得。即使在不同时间加密相同原始数据。

如果在方程（6）中仔细设置参数组和函数，由方程（5）顺序产生的向量 r_j 能避免收敛到平衡解（balanced solution）。

如果密钥是保密的，可以认为在不规则或随机系统加密的数据是难于解密的。本发明的加密系统继承了上述特点。本发明的特征是除了上述惯用加密系统要求的特征外，相关于下列几种情况本发明能自由修改（定制）加密过程。

1.能选择确定依据方程的旋转矩阵 $R_n(\Omega_n)$的表示。

2.在不分散函数值条件基础上能选择地设置方程（6）右侧函数 Ω_n（p,r_{j-1}）和参数 p。

3.各“初始值”可选择地设值。

4.由选择向量的初始值开始，通过选择地重复方程（5）的运行

获得的向量 r_j 可再次设置为用在加密／保密处理中的向量的初始值。

5.当执行具有浮点的运算时，操作结果取决于数字操作处理机和编译器，因此解密处理需要的解密环境相同于加密环境。

依据本实施例的过程能够用整数进行，在该情况下多维空间可由网络分割，并且由离散网格点的坐标表示的向量根据旋转和空间变换改变。

本加密系统的多维旋转向量的加密过程包括许多选择。例如多维向量旋转运行不能简单设置，并且试图解密加密数据的人必须再生旋转产生单元系统，识别该函数系统以规定一个综合的多维向量旋转角，和正确地检测该参数（密钥）。

依据本发明再生向量 r_j 的可能性极低，因为有大量设置非线性函数的方法从具有参数 p（作为密钥）的旋转向量状态获得一旋转角 Ω_n 和大量确定旋转矩阵的方法。

因为本加密系统从小于 n 维旋转矩阵的维数的旋转矩阵产生 n 维旋转矩阵，并应用于连续的处理。还因为依据本发明连续的非线性函数或向量无规则的产生是通过利用n维旋转矩阵在n维空间闭合区定义的n维向量的空间变换和旋转由实数定义的，用选择或数字表示的数据执行加密／解密处理。因此本发明可用在各种应用中。

以下所述为本发明的加密、解密系统在以上所述数据库管理装置的实施例中的应用。

依据本发明一种多维空间旋转系统（多维空间向量系统）用作数据库加密算法。在多维空间旋转系统中连续向量产生在基于预定函数的多维空间，向量分量是加密的密钥流。在多维空间旋转系统中采用具有低特性的各信息处理设备能完成计算。因此系统可应用于便携终端。即，在外部存取本发明数据库的环境下要求加密系统处理数据要成功地保证数据的安全。此时，依据本实施例加密数据库，列密钥不

同于行密钥。因此预定函数的参数使用至少一个列密钥和行密钥确定，由此产生相关于加密的密钥流，于是能产生每行和列的唯一密钥流。

综上所述，依据本发明的数据库管理装置，当加密数据库时检索处理中用的列项使用列项中公用密钥加密，同时其他列项的数据使用各行唯一的行密钥加密。因此相关于不同行使用不同密钥能提高安全性。当执行检索处理时，相关于检索输入的数据使用预定列项中公用列密钥加密，并且将加密的检索数据与加密的数据库比较，从而实现了高速的检索处理。

说 明 书 附 图

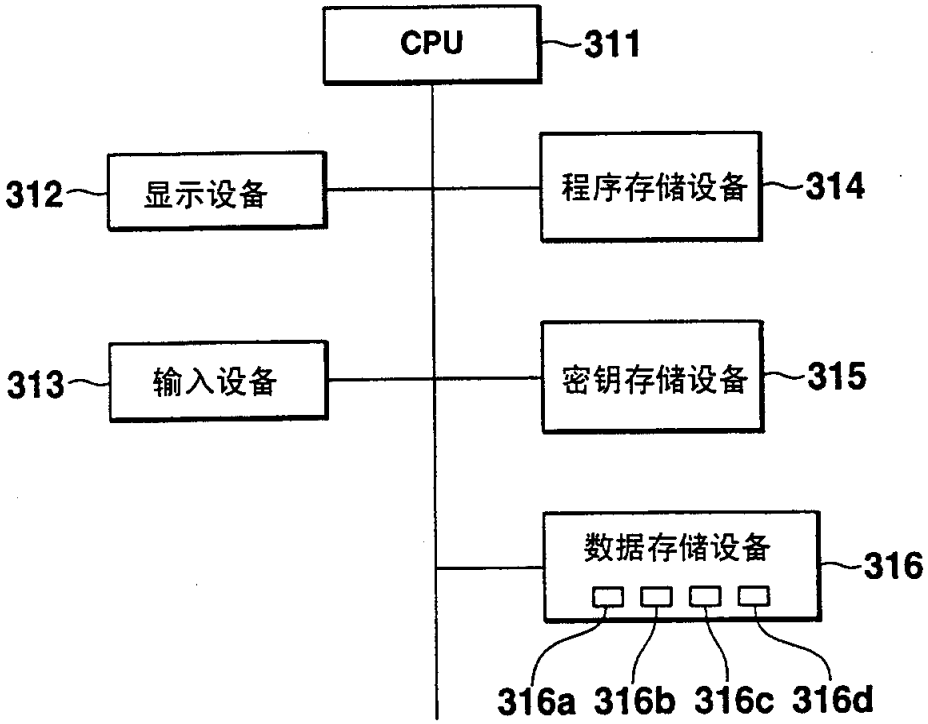

CPU
311
312
显示设备
程序存储设备
314
313
输入设备
密钥存储设备
315
数据存储设备
316
316a
316b
316c
316d

图1

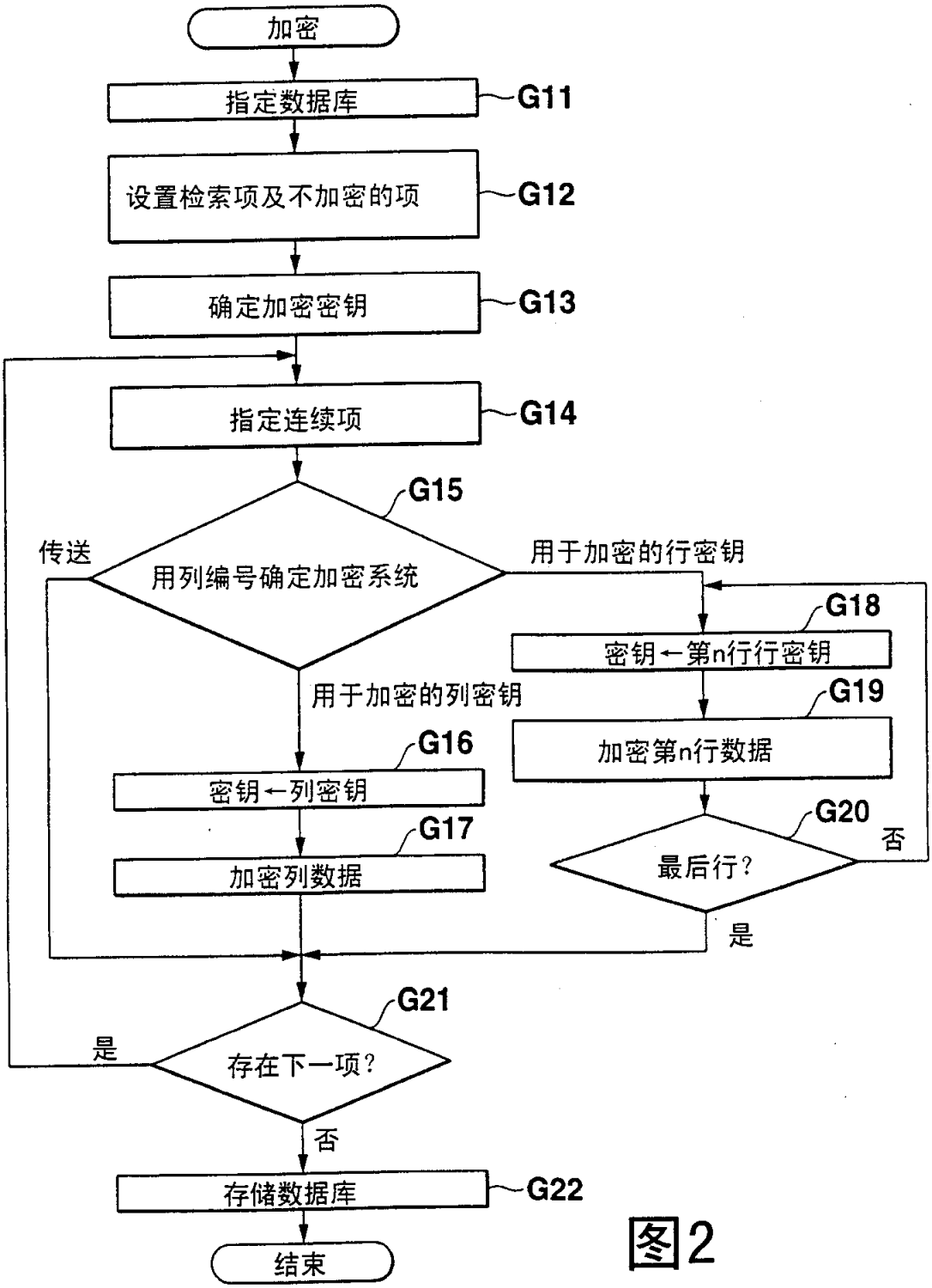

加密
指定数据库
G11
设置检索项及不加密的项
G12
确定加密密钥
G13
指定连续项
G14
G15
传送
用列编号确定加密系统
用于加密的行密钥
用于加密的列密钥
G18
密钥←第n行行密钥
G19
加密第n行数据
G20
最后行?
否
是
G16
密钥←列密钥
G17
加密列数据
G21
是
存在下一项?
否
存储数据库
G22
结束

图2

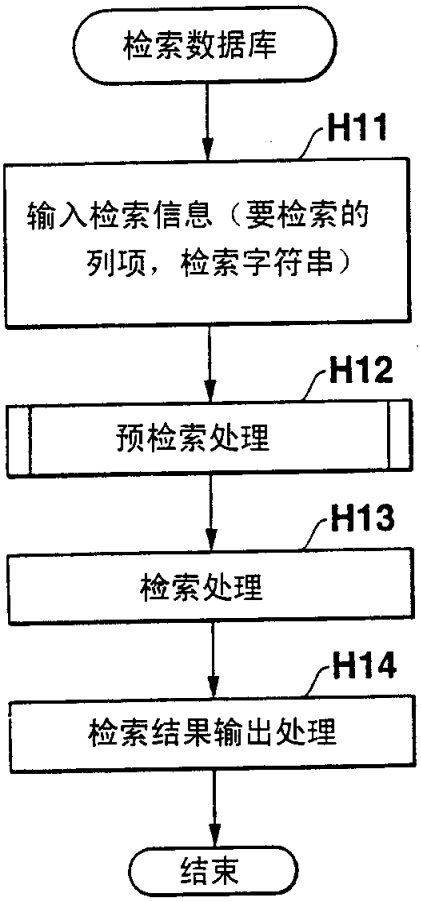

检索数据库
H11
输入检索信息（要检索的列项，检索字符串）
H12
预检索处理
H13
检索处理
H14
检索结果输出处理
结束

图3A

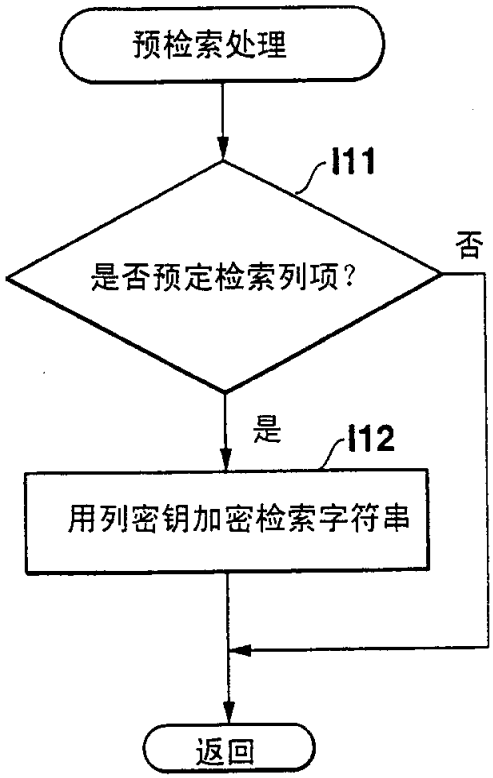

预检索处理
I11
是否预定检索列项？
否
是
I12
用列密钥加密检索字符串
返回

图3B

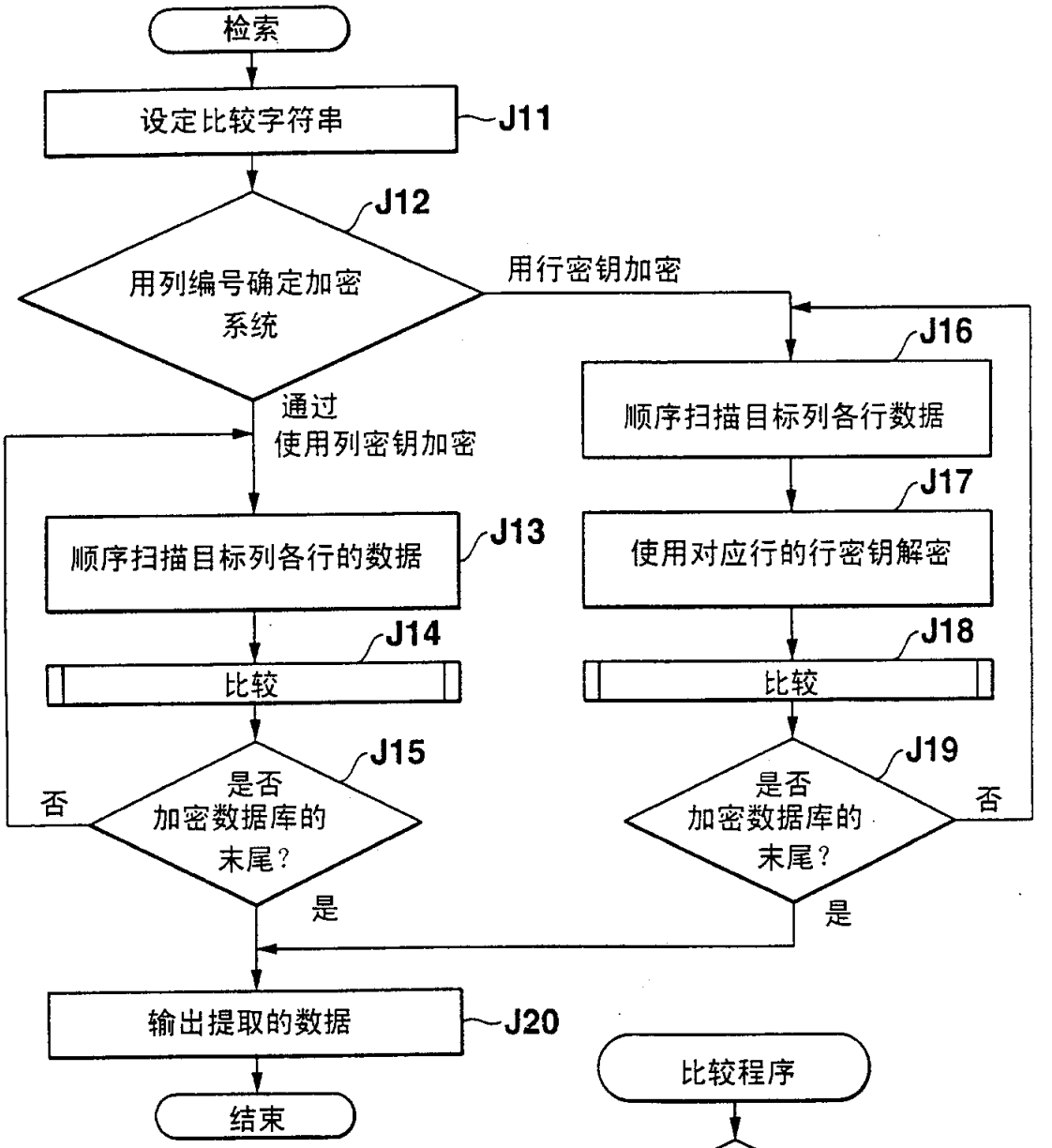

检索
设定比较字符串
J11
J12
用列编号确定加密系统
用行密钥加密
通过
使用列密钥加密
J16
顺序扫描目标列各行数据
J17
顺序扫描目标列各行的数据
J13
使用对应行的行密钥解密
J14
比较
J18
比较
J15
是否加密数据库的末尾？
否
J19
是否加密数据库的末尾？
否
是
是
输出提取的数据
J20
结束

图4A

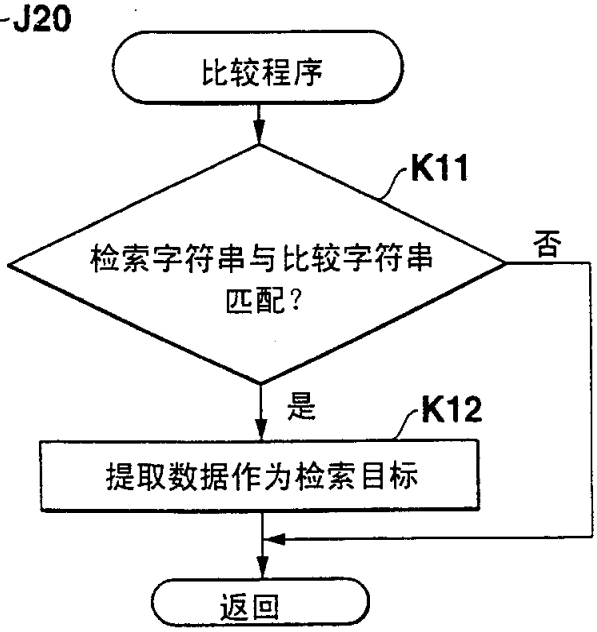

比较程序
K11
检索字符串与比较字符串匹配？
否
是
K12
提取数据作为检索目标
返回

图4B

(a)

编号	姓 名	州	体重	身高	年龄	电话
1	约 翰	纽 约	63	130	22	407-228-6611
2	克利斯	佛罗里达	72	190	21	123-456-7890
3	迈克尔	明尼苏达	65	163	27	101-202-3030
4	大 卫	衣 阿 华	63	145	34	523-761-0045
5	马 克	纽 约	65	152	30	832-962-9001
6	丹尼尔	衣 阿 华	68	170	25	231-981-9454
7	乔 治	爱 达 荷	69	180	31	561-545-4389
8	亨 利	佛罗里达	71	165	22	239-203-9800
9	乔	新 泽 西	66	163	27	239-129-9898

加密 列密钥
行密钥

(b)

编号	姓 名	州	体重	身高	年龄	电话
1	WJls	noevjolc	qw	ywe	jh	igdltytfhDSK
2	ddGGa	h*/fDD	lr	Erw	hg	LKtYtDSkoKOW
3	1jkjl+P	gah{6×pVd	RK	Tyi	tY	hkliiydageQK
4	3ek@s	kHHs	kd	DHH	Kl	k+fDlKnBerJf
5	erlN	noevjoic	jD	iOO	Gv	wsdERfvW2Sdf
6	F>sSlu	kHHS	8u	lki	ij	1×cVlmFmkjpo
7	(:ld?k	lJHFD	HH	lpa	LK	kjwDkJGvfDoa
8	rhJKd	h*/fDD	ew	Aii	jh	e419h-ka+qwH
9	ifd	ASoChijlO-	Df	1ky	tY	qLFUiCVkj@kl

解密 列密钥
行密钥

(c)

编号	姓 名	州	体重	身高	年龄	电话
1	约 翰	纽 约	63	130	22	407-228-6611
2	克利斯	佛罗里达	72	190	21	123-456-7890
3	迈克尔	明尼苏达	65	163	27	101-202-3030
4	大 卫	衣 阿 华	63	145	34	523-761-0045
5	马 克	纽 约	65	152	30	832-962-9001
6	丹尼尔	衣 阿 华	68	170	25	231-981-9454
7	乔 治	爱 达 荷	69	180	31	561-545-4389
8	亨 利	佛罗里达	71	165	22	239-203-9800
9	乔	新 泽 西	66	163	27	239-129-9898

图5

列密钥

编号	姓名	州	体重	身高	年龄	电话
无	“苹果”	“桔子”	行密钥	行密钥	“柠檬”	行密钥

行密钥

编号	
1	“虎”
2	“狗”
3	“猫”
4	“老鼠”
5	“象”
6	“母牛”
7	“猪”
8	“兔”
9	“狮子”

图6

00.10.29

(a)

编号	姓 名	州	体重	身高	年龄	电话
1	约 翰	纽 约	63	130	22	407-228-6611
2	克利斯	佛罗里达	72	190	21	123-456-7890
3	迈克尔	明尼苏达	65	163	27	101-202-3030
4	大 卫	衣 阿 华	63	145	34	523-761-0045
5	马 克	纽 约	65	152	30	832-962-9001
6	丹尼尔	衣 阿 华	68	170	25	231-981-9454
7	乔 治	爱 达 荷	69	180	31	561-545-4389
8	亨 利	佛罗里达	71	165	22	239-203-9800
9	乔	新 泽 西	66	163	27	239-129-9898

加密 组合密钥

(b)

编号	姓 名	州	体重	身高	年龄	电话
1	WJls	noevjolc	xo	qwe	jh	dfghaj;lkqlu
2	ddGGa	h*/fDD	wi	klA	hg	qwTylBnDFiKj
3	1jkjl+P	gah{6×pVd	hi	lKJ	tY	DafgiqikimD-
4	3ek@s	kHHs	s?	SGA	Kl	hi*khaTygfXd
5	erlN	noevjoic	d-	ASD	Gv	8uyDBmAkolka
6	F>sSlu	kHHS	1*	qoK	ij	jhtvbnMKJASW
7	(:ld?k	lJHFD	df	sLL	LK	lQwSRyuiokjq
8	rhJKd	h*/fDD	Ws	tyH	of	Dfha*kaqil
9	ifd	ASoChijlO-	qo	H2a	tY	lkjHYAGoiuq

解密 组合密钥

(c)

编号	姓 名	州	体重	身高	年龄	电话
1	约 翰	纽 约	63	130	22	407-228-6611
2	克利丝	佛罗里达	72	190	21	123-456-7890
3	迈克尔	明尼苏达	65	163	27	101-202-3030
4	大 卫	衣 阿 华	63	145	34	523-761-0045
5	马 克	纽 约	65	152	30	832-962-9001
6	丹尼尔	衣 阿 华	68	170	25	231-981-9454
7	乔 治	爱 达 荷	69	180	31	561-545-4389
8	亨 利	佛罗里达	71	165	22	239-203-9800
9	乔	新 泽 西	66	163	27	239-129-9898

图7

编号	姓　名	州	体重	身高	年龄	电话
无	“苹果”	“桔子”	“香蕉虎”	“荔枝”	“柠檬”	“杏虎”
无	“苹果”	“桔子”	“香蕉狗”	“荔枝”	“柠檬”	“杏狗”
无	“苹果”	“桔子”	“香蕉猫”	“荔枝”	“柠檬”	“杏猫”
无	“苹果”	“桔子”	“香蕉老鼠”	“荔枝”	“柠檬”	“杏老鼠”
无	“苹果”	“桔子”	“香蕉象”	“荔枝”	“柠檬”	“杏象”
无	“苹果”	“桔子”	“香蕉母牛”	“荔枝”	“柠檬”	“杏母牛”
无	“苹果”	“桔子”	“香蕉猪”	“荔枝”	“柠檬”	“杏猪”
无	“苹果”	“桔子”	“香蕉兔”	“荔枝”	“柠檬”	“杏兔”
无	“苹果”	“桔子”	“香蕉狮子”	“荔枝”	“柠檬”	“杏狮子”

列密钥

编码	姓名	州	体重	身高	年龄	电话
无	“苹果”	“桔子”	“香蕉”＋行密钥	“荔枝”＋行密钥	“柠檬”	“杏”＋行密钥

编号	
1	“虎”
2	“狗”
3	“猫”
4	“老鼠”
5	“象”
6	“母牛”
7	“猪”
8	“兔”
9	“狮子”

图8

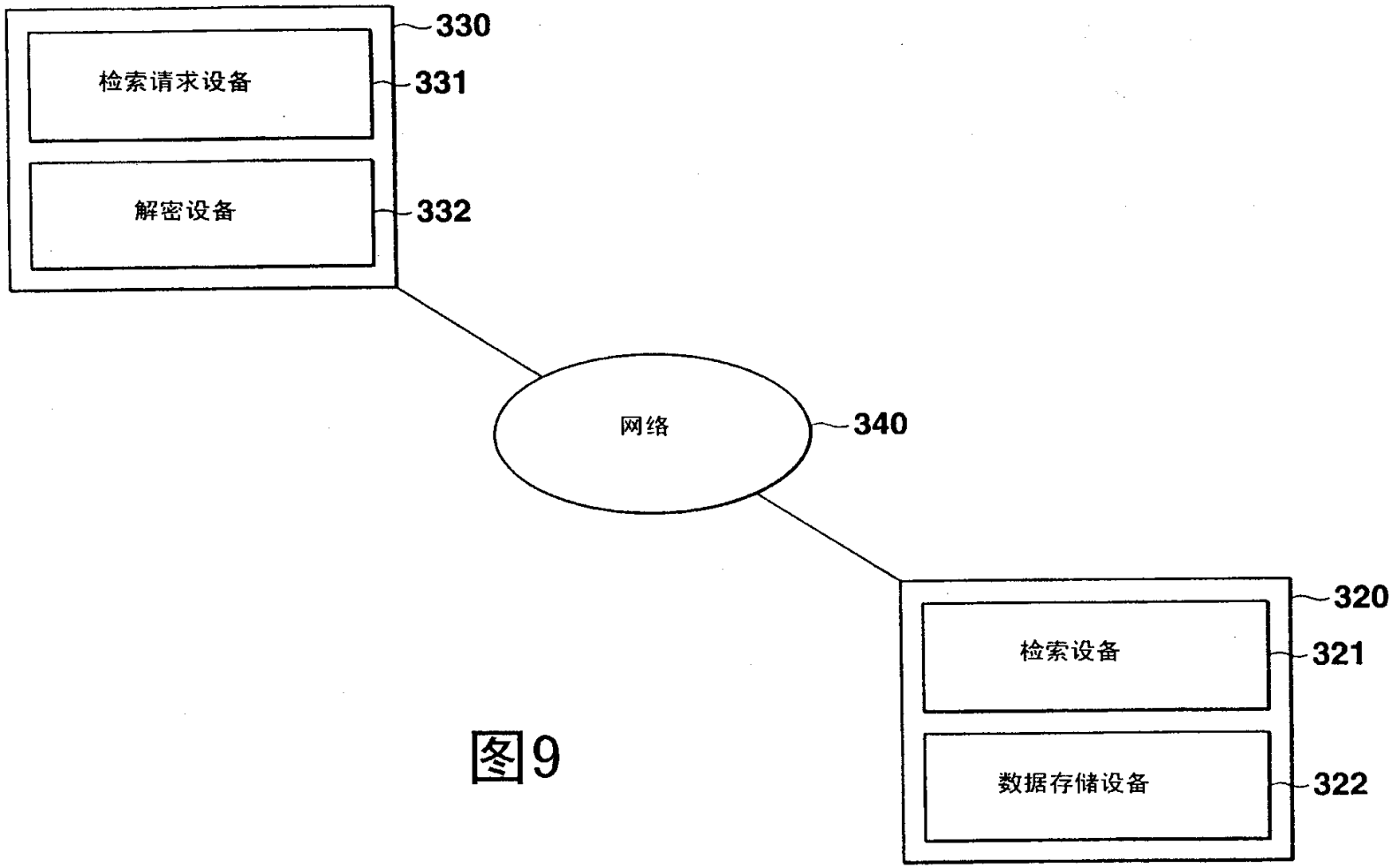


图9

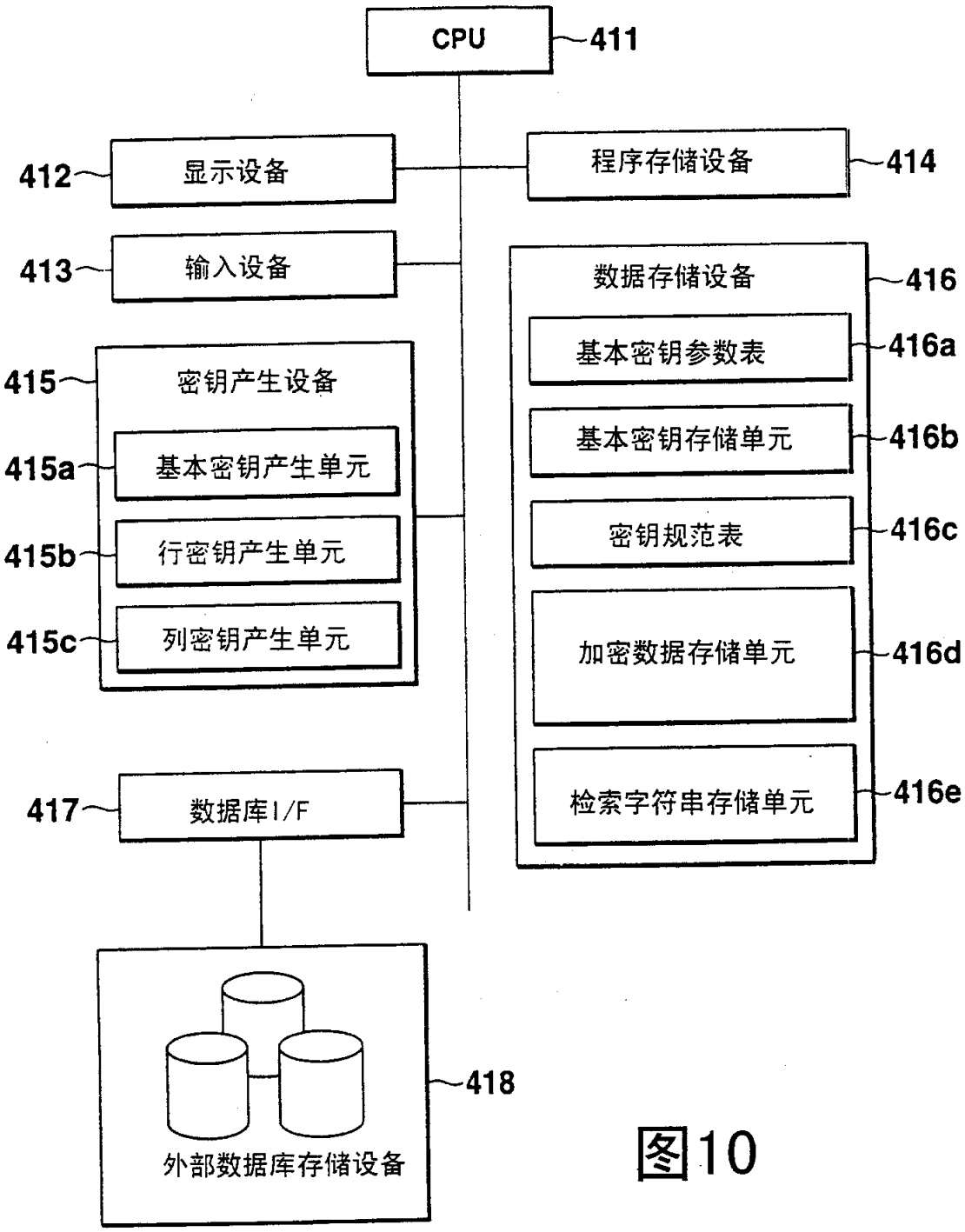

CPU
411
412
显示设备
程序存储设备
414
413
输入设备
数据存储设备
416
基本密钥参数表
416a
415
密钥产生设备
基本密钥存储单元
416b
415a
基本密钥产生单元
密钥规范表
416c
415b
行密钥产生单元
加密数据存储单元
416d
415c
列密钥产生单元
检索字符串存储单元
416e
417
数据库I/F
418
外部数据库存储设备

图10

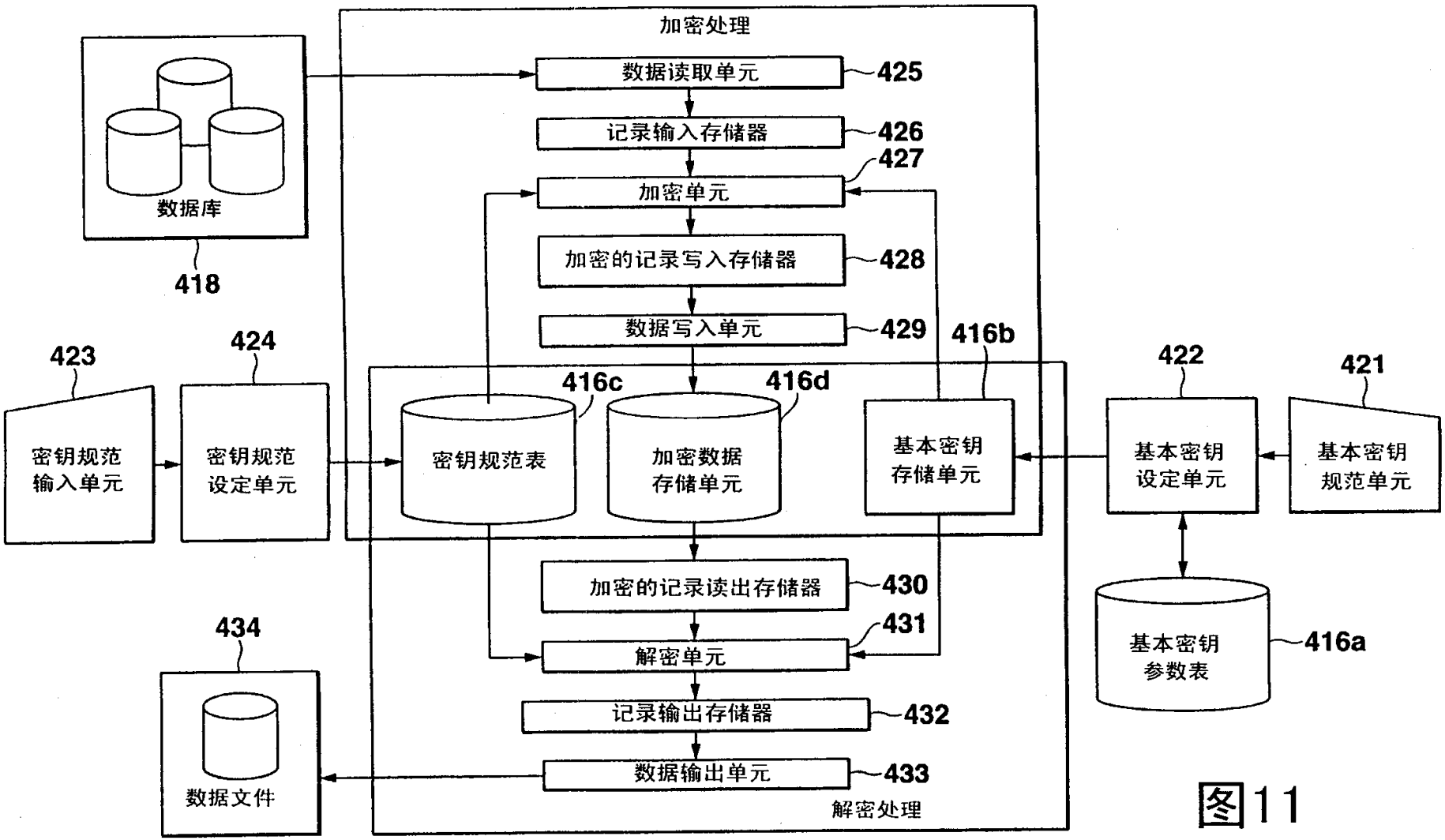

加密处理
数据读取单元
425
记录输入存储器
426
427
加密单元
加密的记录写入存储器
428
数据写入单元
429
416b
数据库
418
423
424
密钥规范
输入单元
密钥规范
设定单元
416c
416d
密钥规范表
加密数据
存储单元
基本密钥
存储单元
422
421
基本密钥
设定单元
基本密钥
规范单元
加密的记录读出存储器
430
431
解密单元
434
基本密钥
参数表
416a
记录输出存储器
432
数据输出单元
433
数据文件
解密处理

图11

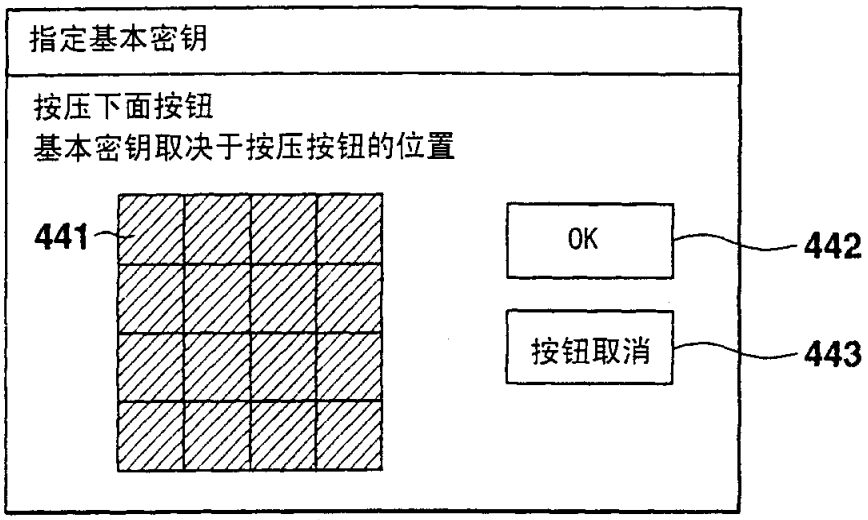


图12

基本密钥参数表

按钮位置	基本参数值
1	5
2	7
3	9
4	11
5	13
6	15
7	17
8	19
9	21
10	23
11	25
12	27
13	29
14	31
15	33
16	35

416a

图13

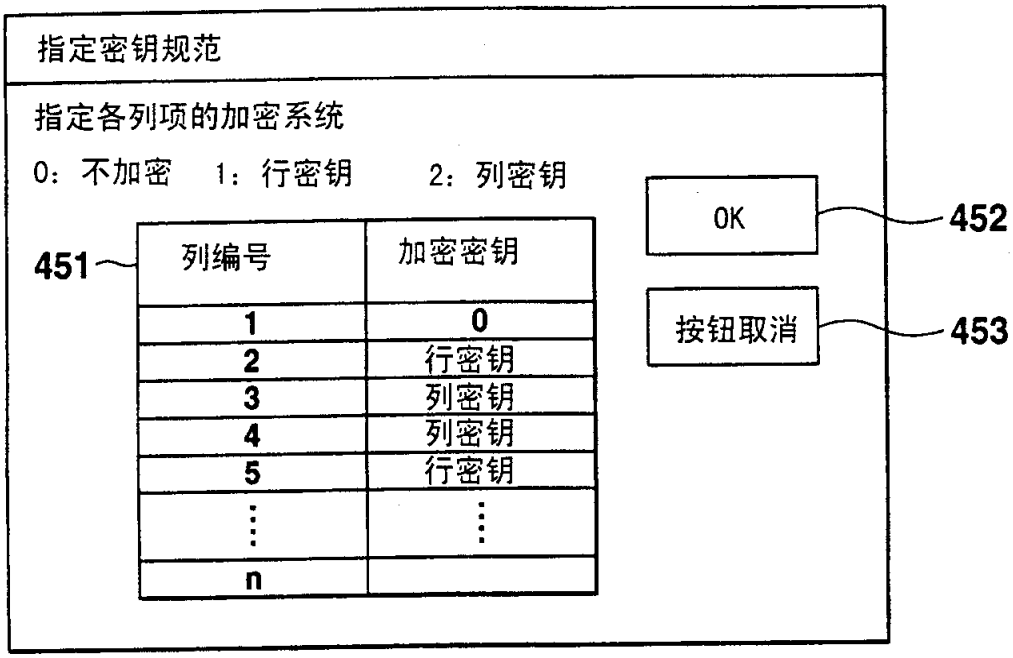


图14

密钥规范表

列名称	列编号	加密密钥
（编号）	1	0
（姓名）	2	行密钥
（州）	3	列密钥
（年龄）	4	列密钥
（电话）	5	行密钥

416c

图15

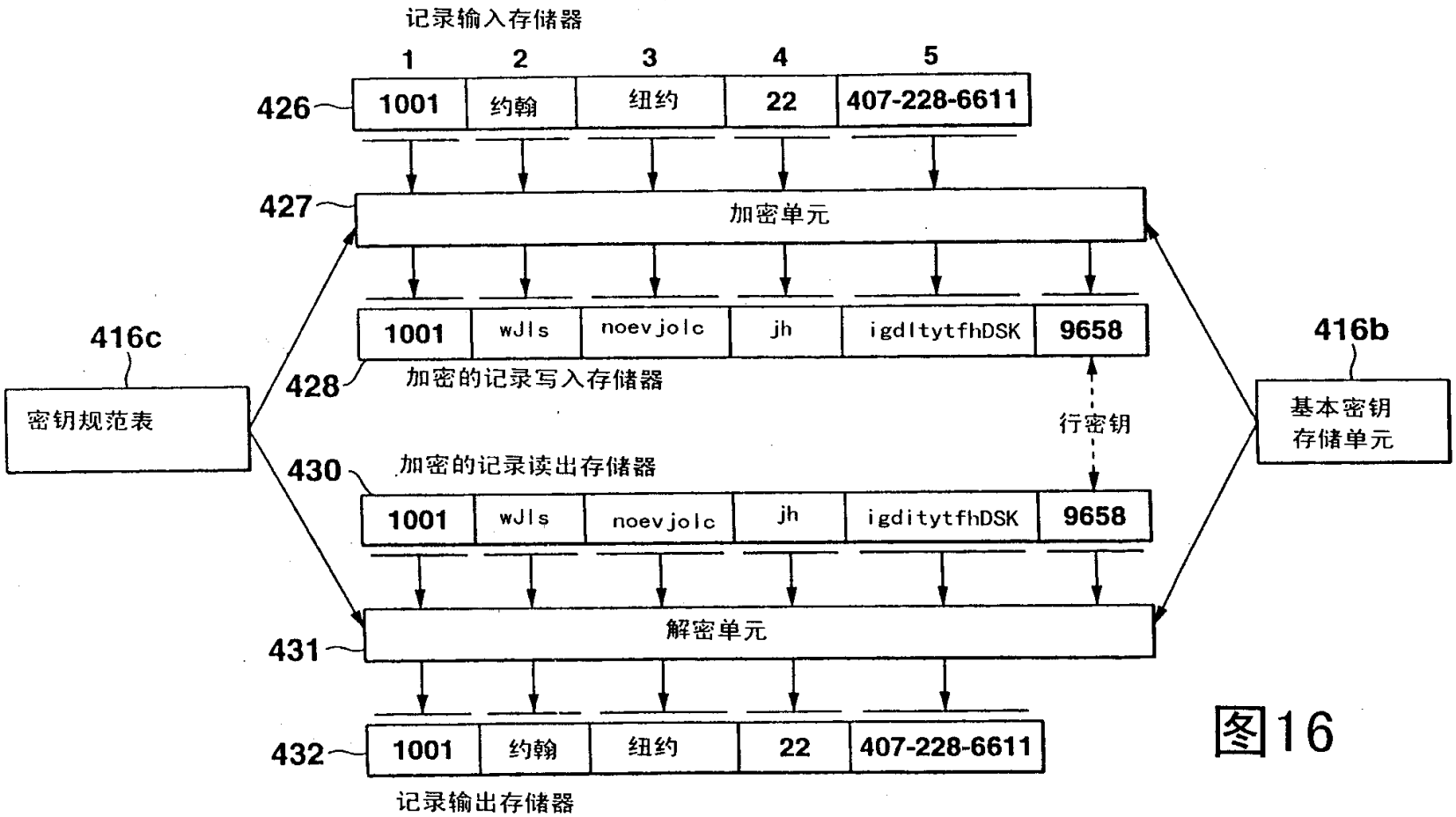

记录输入存储器
1
2
3
4
5
426
1001
约翰
纽约
22
407-228-6611
427
加密单元
1001
wJls
noevjolc
jh
igdltytfhDSK
9658
428
加密的记录写入存储器
416c
密钥规范表
416b
基本密钥
存储单元
行密钥
430
加密的记录读出存储器
1001
wJls
noevjolc
jh
igditytfhDSK
9658
431
解密单元
432
1001
约翰
纽约
22
407-228-6611
记录输出存储器

图16

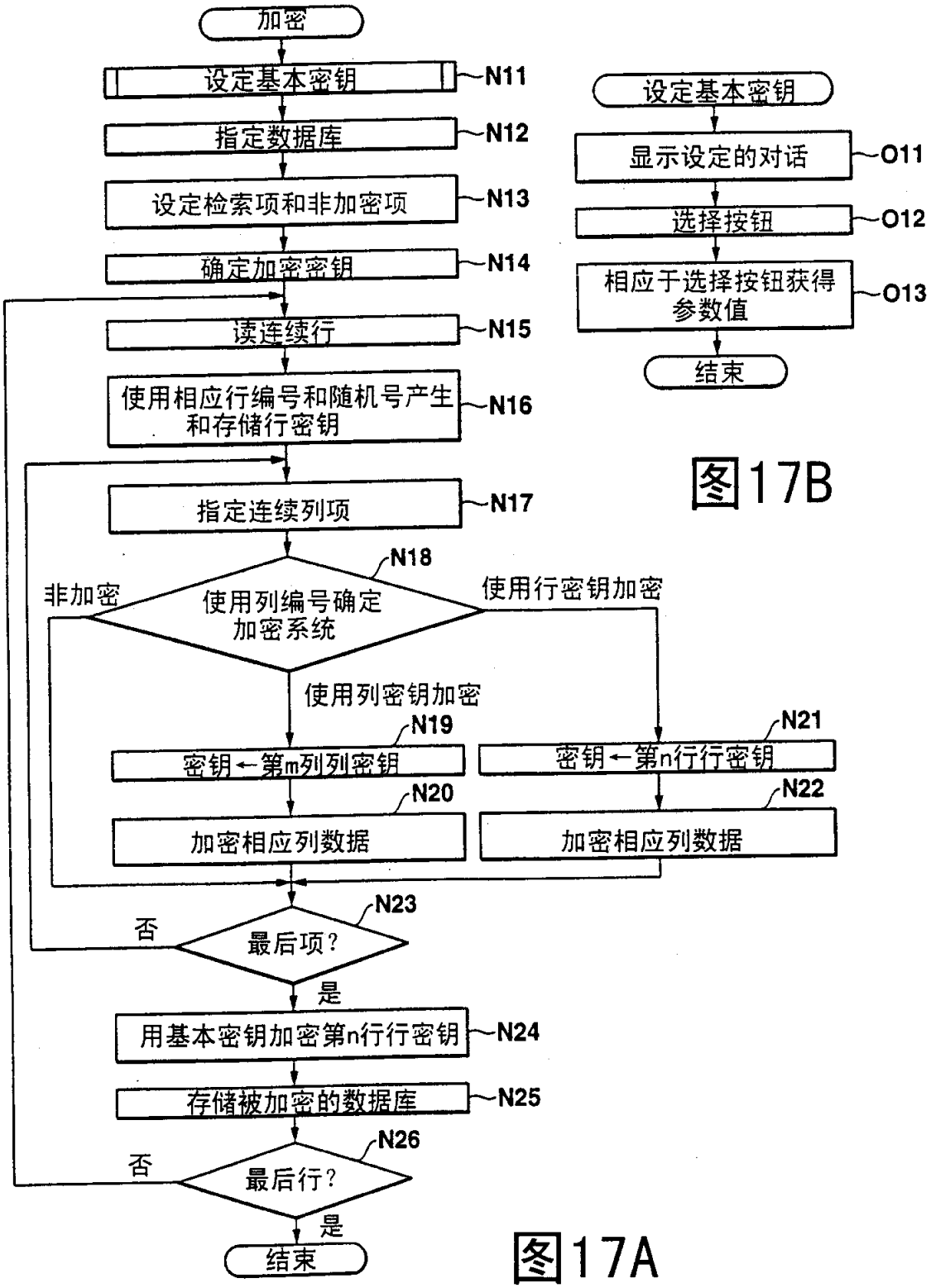

加密
设定基本密钥
N11
指定数据库
N12
设定检索项和非加密项
N13
确定加密密钥
N14
读连续行
N15
使用相应行编号和随机号产生和存储行密钥
N16
指定连续列项
N17
N18
非加密
使用列编号确定加密系统
使用行密钥加密
使用列密钥加密
N19
密钥←第m列列密钥
N20
加密相应列数据
N21
密钥←第n行行密钥
N22
加密相应列数据
N23
否
最后项?
是
用基本密钥加密第n行行密钥
N24
存储被加密的数据库
N25
N26
否
最后行?
是
结束
设定基本密钥
显示设定的对话
O11
选择按钮
O12
相应于选择按钮获得参数值
O13
结束

图17B

图17A

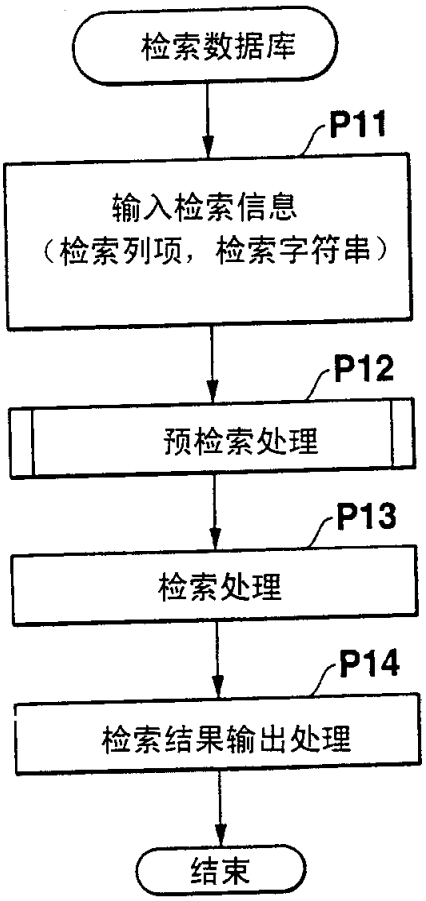

检索数据库
P11
输入检索信息
（检索列项，检索字符串）
P12
预检索处理
P13
检索处理
P14
检索结果输出处理
结束

图18A

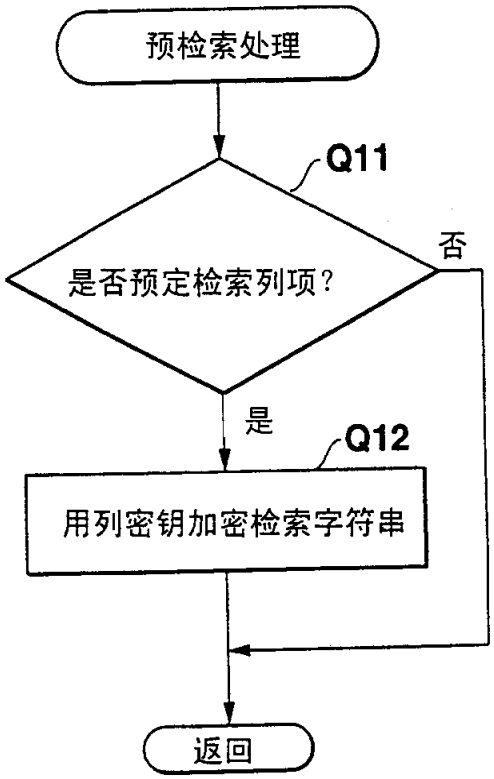

预检索处理
Q11
是否预定检索列项？
否
是
Q12
用列密钥加密检索字符串
返回

图18B

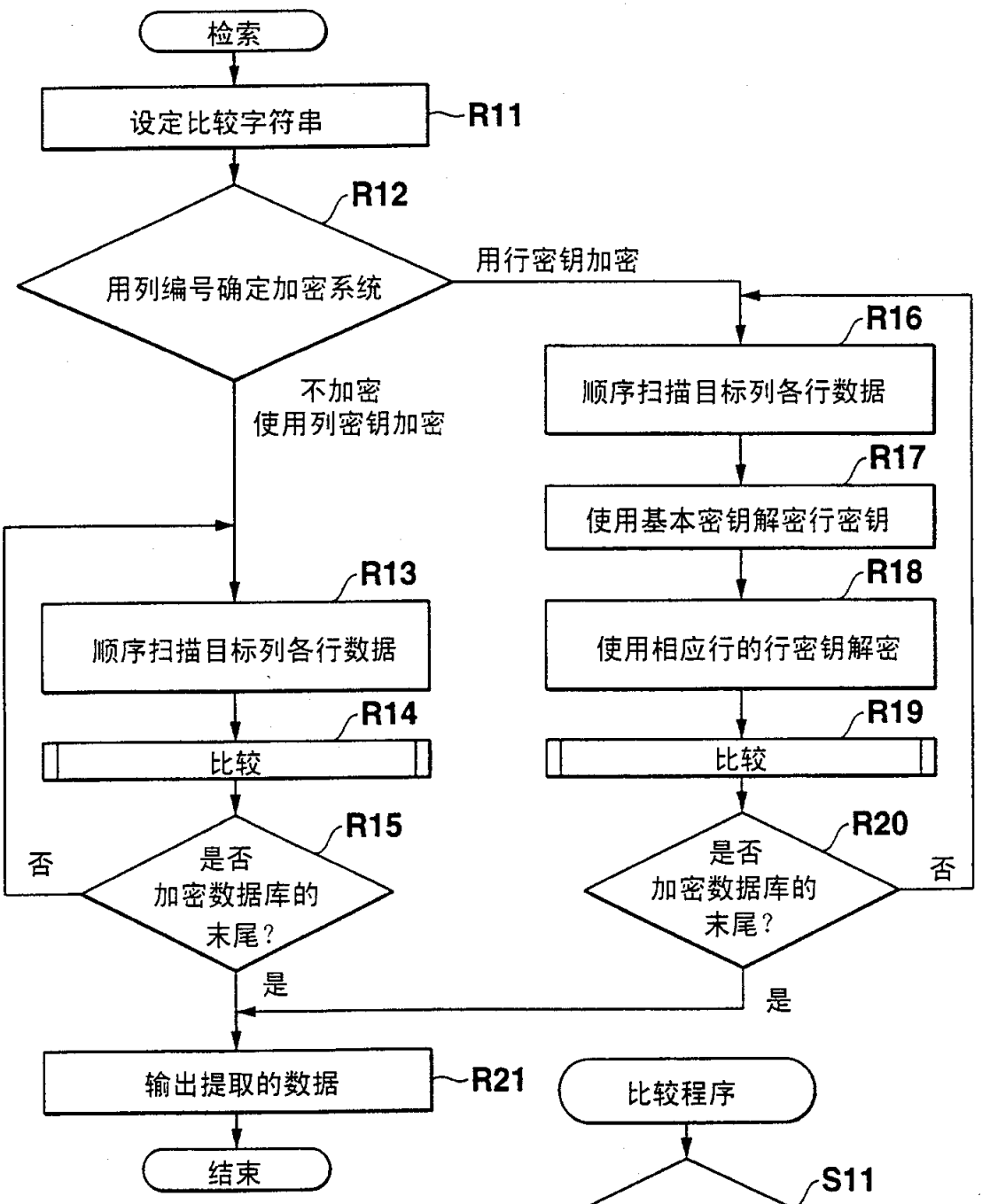

检索
设定比较字符串
R11
R12
用列编号确定加密系统
用行密钥加密
不加密
使用列密钥加密
R16
顺序扫描目标列各行数据
R17
使用基本密钥解密行密钥
R13
顺序扫描目标列各行数据
R18
使用相应行的行密钥解密
R14
比较
R19
比较
R15
是否
加密数据库的
末尾?
否
R20
是否
加密数据库的
末尾?
否
是
是
输出提取的数据
R21
结束

图19A

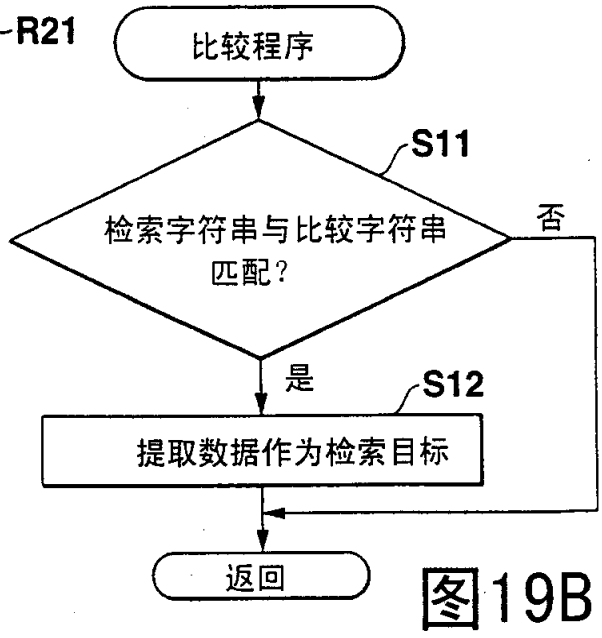

比较程序
S11
检索字符串与比较字符串
匹配?
否
是
S12
提取数据作为检索目标
返回

图19B

00.10.29

(a)

编号	姓 名	州	年龄	电话
1001	约 翰	纽 约	22	407-228-6611
1002	克利斯	佛罗里达	21	123-456-7890
1003	迈克尔	明尼苏达	27	101-202-3030
1004	大 卫	衣 阿 华	34	523-761-0045
1005	马 克	纽 约	30	832-962-9001
1006	丹尼尔	衣 阿 华	25	231-981-9454
1007	乔 治	爱 达 荷	31	561-545-4389
1008	亨 利	佛罗里达	22	239-203-9800
1009	乔	新 泽 西	27	239-129-9898

加密 列密钥 行密钥

(b)

编号	姓 名	州	年龄	电话	链接密钥
1001	WJIs	noevjolc	jh	igdltytfhDSK	9658
1002	ddGGa	h*/fDD	hg	LKtYtDSkoKOW	9143
1003	1jkjl+P	gah{6×pVd	tY	hkliiydageQK	8278
1004	3ek@s	kHHs	Kl	k+fDlKnBerJf	4358
1005	erlN	noevjoic	Gv	wsdERfvW2Sdf	5784
1006	F>sSlu	kHHS	ij	1×cVlmFmkjpo	9743
1007	(:ld?k	lJHFD	LK	kjwDkJGvfDoa	3935
1008	rhJKd	h*/fDD	jh	e419h-ka+qwH	7412
1009	ifd	ASoChijlO-	tY	qLFUiCVkj@kl	9593

解密 列密钥 行密钥

(c)

编号	姓 名	州	年龄	电话
1001	约 翰	纽 约	22	407-228-6611
1002	克利斯	佛罗里达	21	123-456-7890
1003	迈克尔	明尼苏达	27	101-202-3030
1004	大 卫	衣 阿 华	34	523-761-0045
1005	马 克	纽 约	30	832-962-9001
1006	丹尼尔	衣 阿 华	25	231-981-9454
1007	乔 治	爱 达 荷	31	561-545-4389
1008	亨 利	佛罗里达	22	239-203-9800
1009	乔	新 泽 西	27	239-129-9898

图20

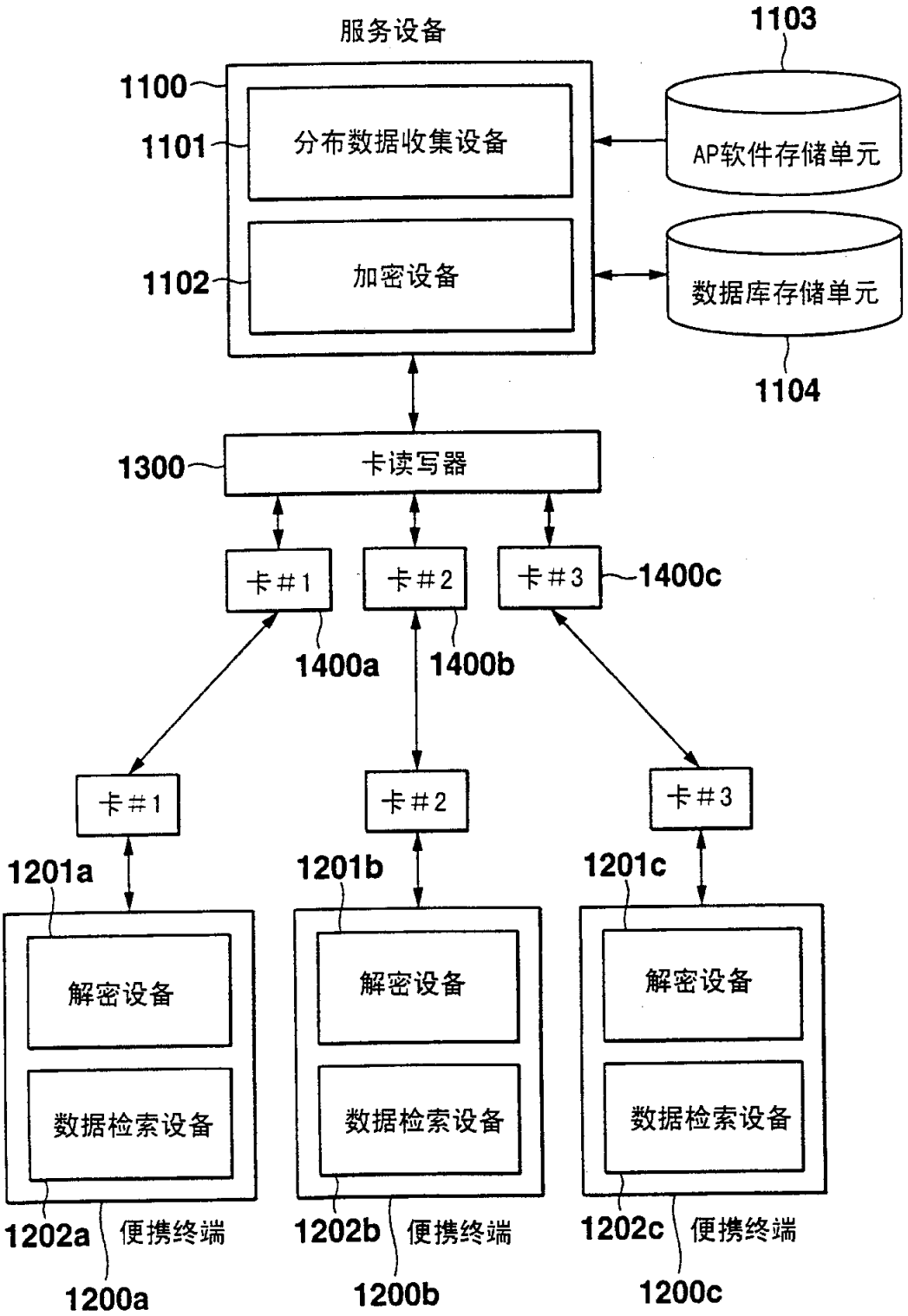

服务设备
1100
1101
分布数据收集设备
1102
加密设备
1103
AP软件存储单元
数据库存储单元
1104
1300
卡读写器
卡#1
卡#2
卡#3
1400c
1400a
1400b
卡#1
卡#2
卡#3
1201a
1201b
1201c
解密设备
数据检索设备
解密设备
数据检索设备
解密设备
数据检索设备
1202a
便携终端
1200a
1202b
便携终端
1200b
1202c
便携终端
1200c

图21

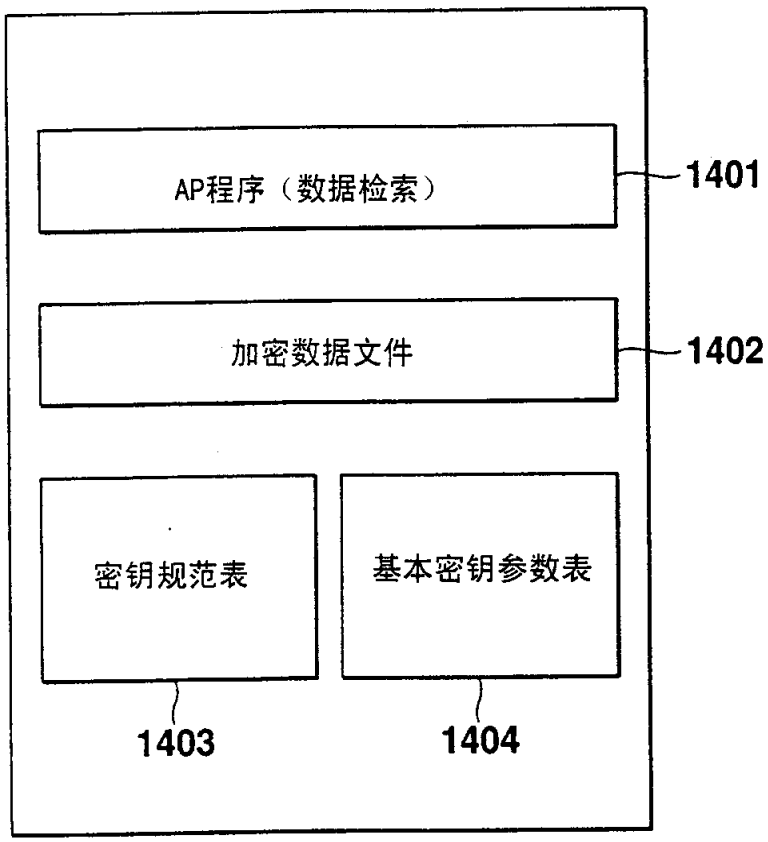


图22

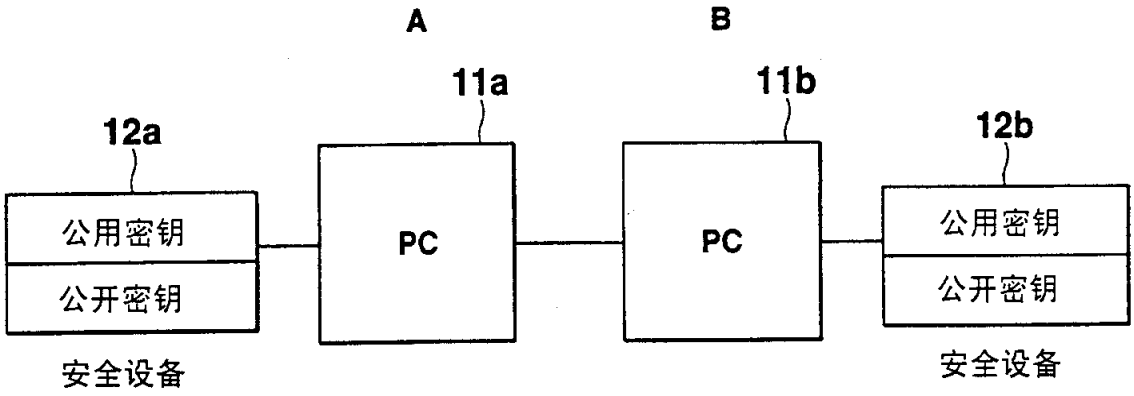


图23

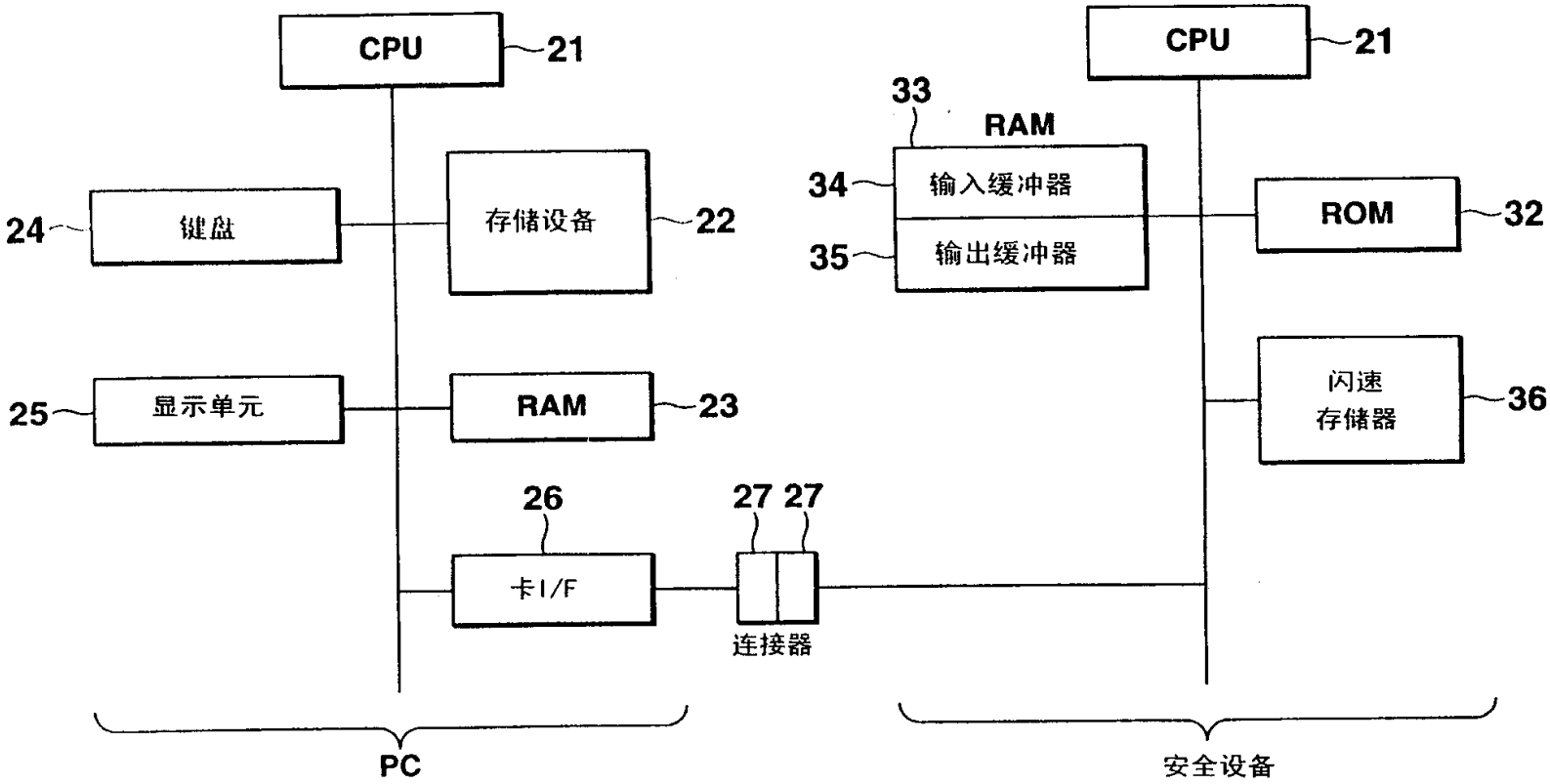

CPU
21
24
键盘
存储设备
22
25
显示单元
RAM
23
26
卡I/F
27 27
连接器
PC
CPU
21
33
RAM
34
输入缓冲器
35
输出缓冲器
ROM
32
闪速
存储器
36
安全设备

图24

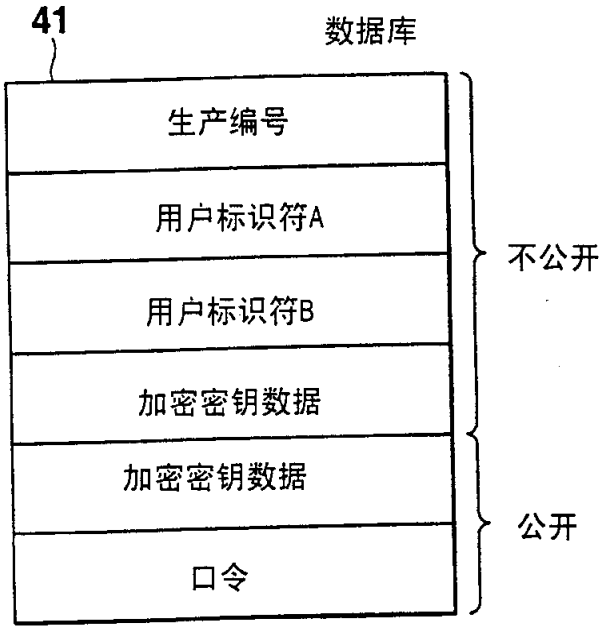


图25

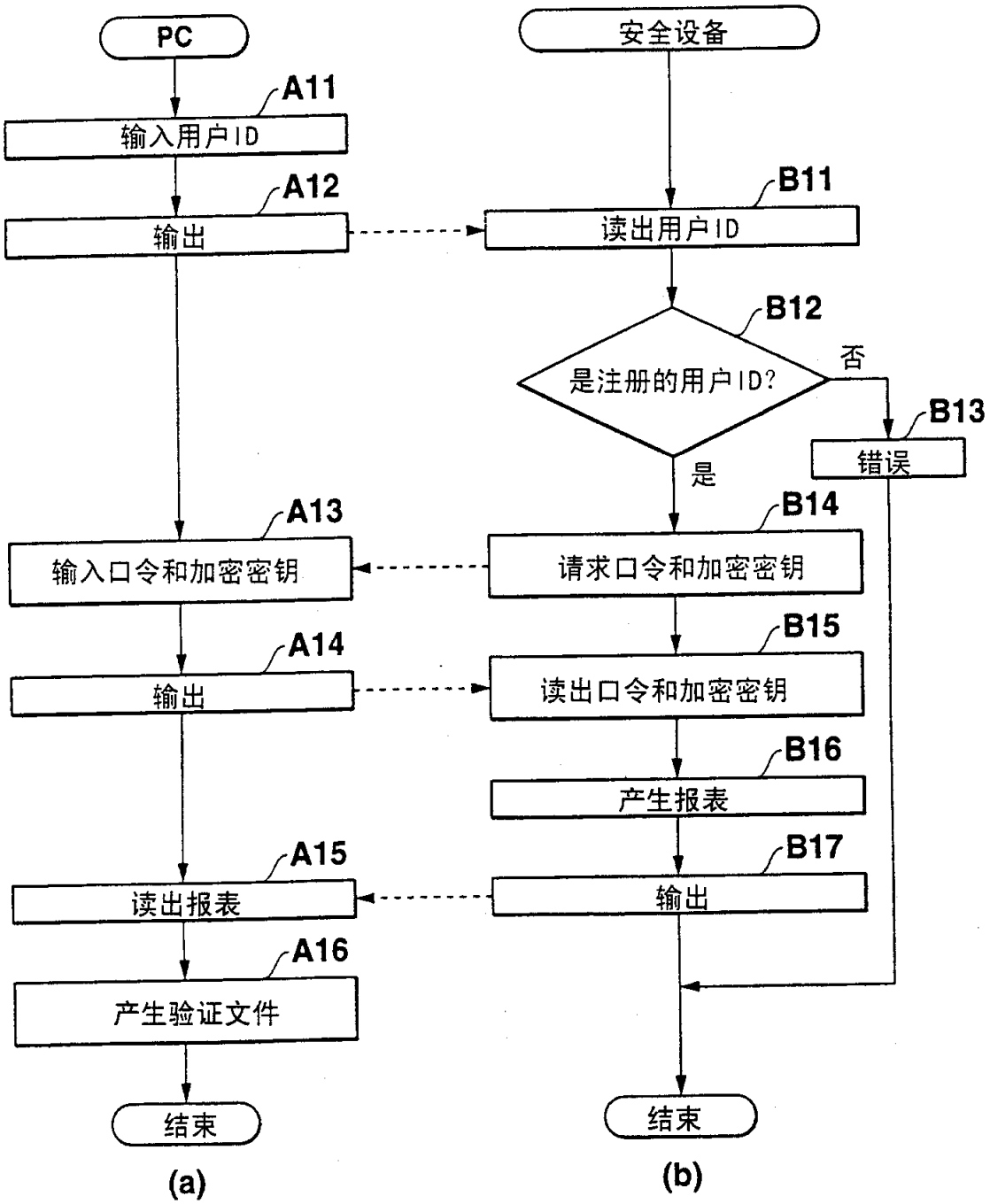

PC
A11
输入用户ID
A12
输出
A13
输入口令和加密密钥
A14
输出
A15
读出报表
A16
产生验证文件
结束
(a)
安全设备
B11
读出用户ID
B12
是注册的用户ID?
否
是
B13
错误
B14
请求口令和加密密钥
B15
读出口令和加密密钥
B16
产生报表
B17
输出
结束
(b)

图26

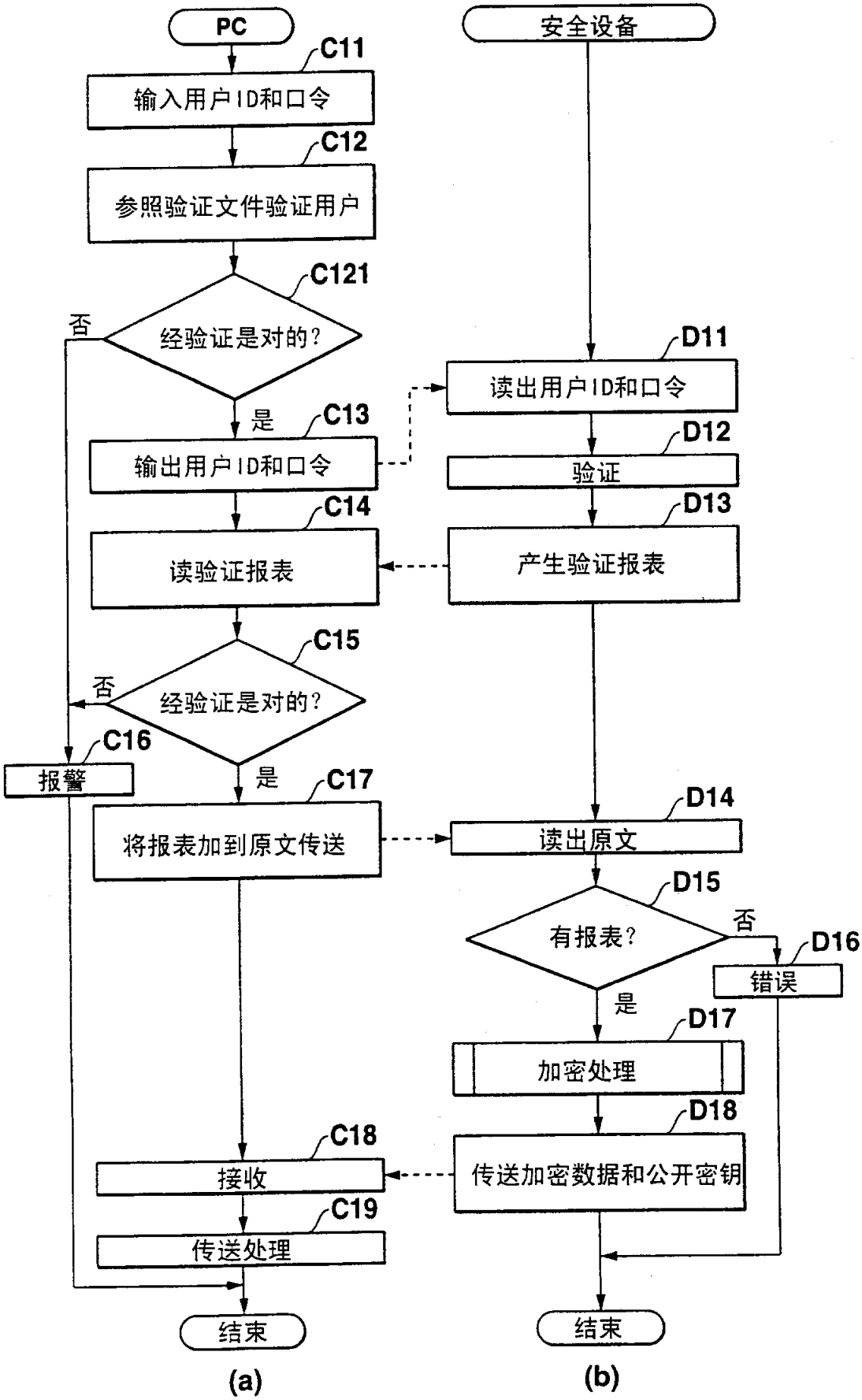

PC
C11
输入用户ID和口令
C12
参照验证文件验证用户
C121
经验证是对的?
否
是
C13
输出用户ID和口令
C14
读验证报表
C15
经验证是对的?
否
C16
报警
是
C17
将报表加到原文传送
C18
接收
C19
传送处理
结束
(a)
安全设备
D11
读出用户ID和口令
D12
验证
D13
产生验证报表
D14
读出原文
D15
有报表?
否
D16
错误
是
D17
加密处理
D18
传送加密数据和公开密钥
结束
(b)

图27

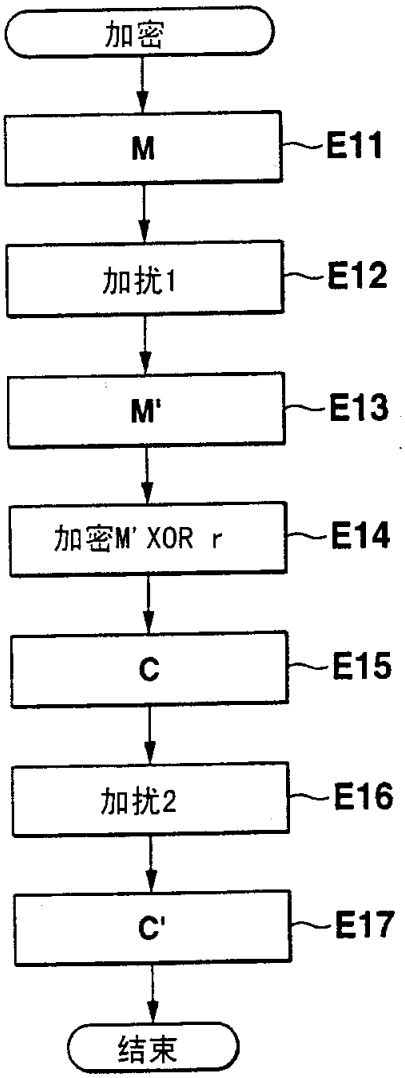

加密
M
E11
加扰1
E12
M'
E13
加密M' XOR r
E14
C
E15
加扰2
E16
C'
E17
结束

图28A

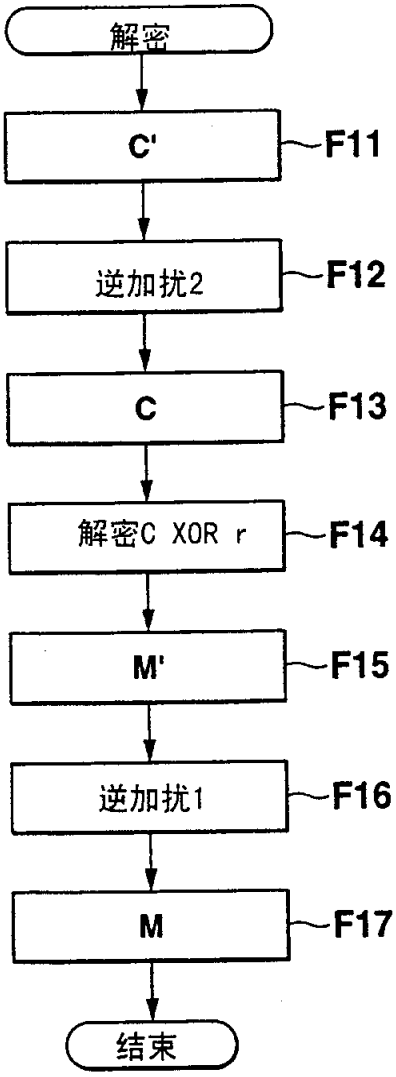

解密
C'
F11
逆加扰2
F12
C
F13
解密C XOR r
F14
M'
F15
逆加扰1
F16
M
F17
结束

图28B

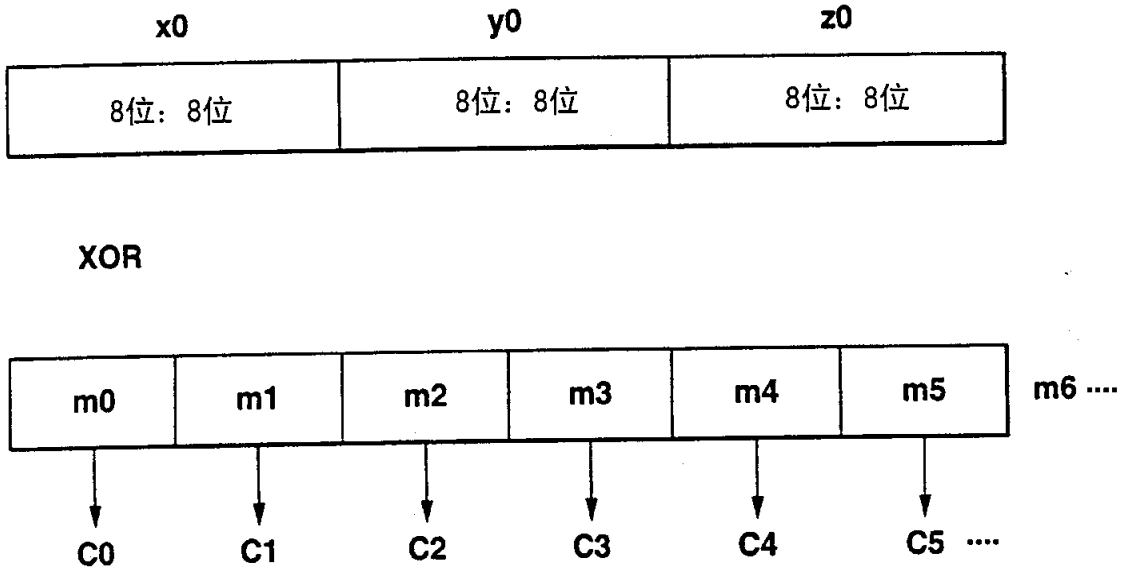


图29

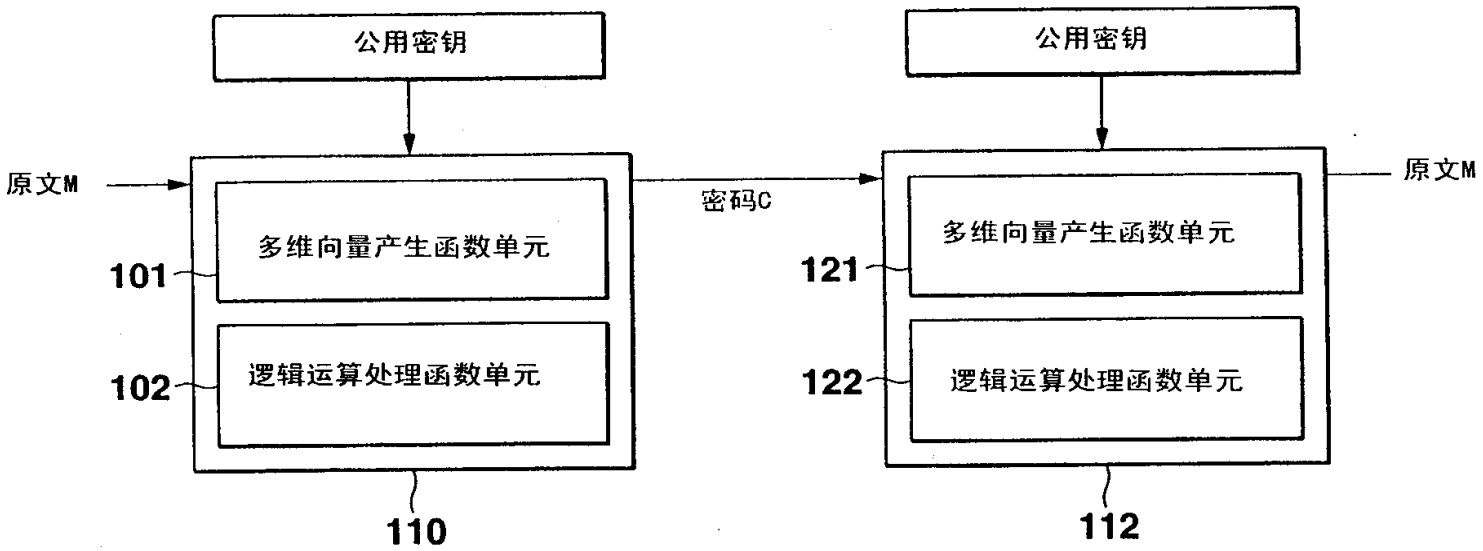

公用密钥
原文M
多维向量产生函数单元
101
逻辑运算处理函数单元
102
110
密码C
公用密钥
原文M
多维向量产生函数单元
121
逻辑运算处理函数单元
122
112

图30

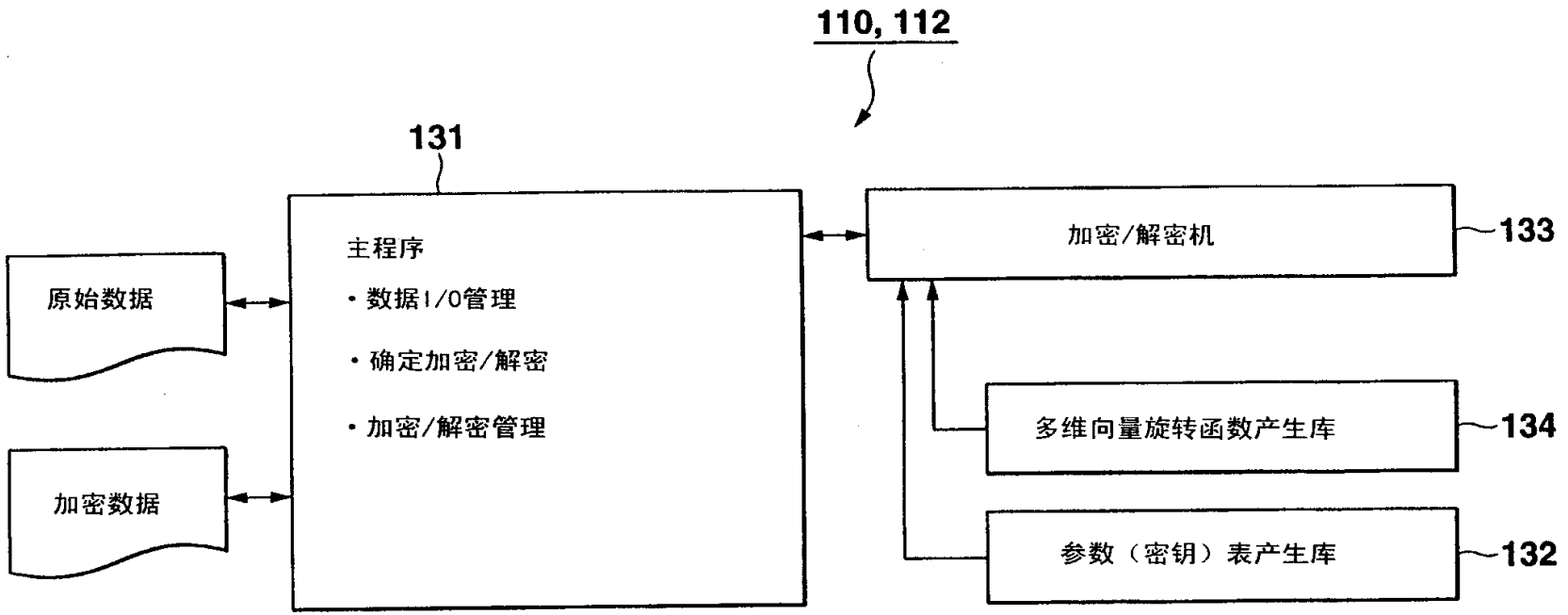

110, 112
131
主程序
• 数据I/O管理
• 确定加密/解密
• 加密/解密管理
原始数据
加密数据
加密/解密机
133
多维向量旋转函数产生库
134
参数（密钥）表产生库
132

图31

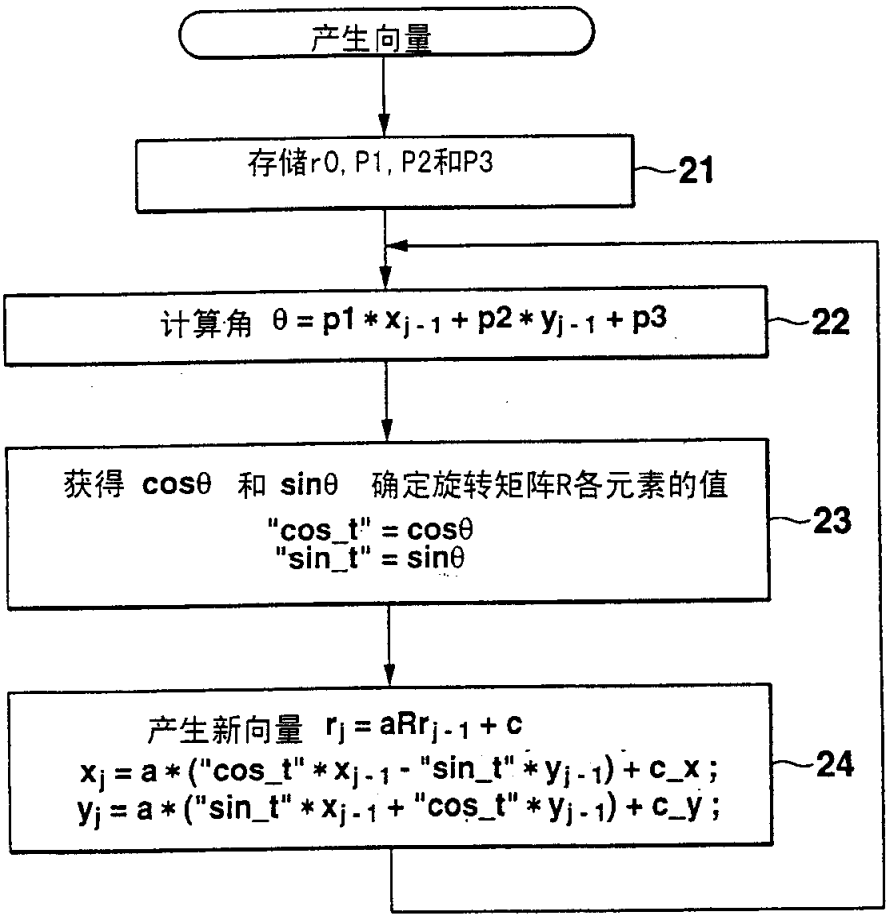

产生向量
存储r0, P1, P2和P3
21
计算角 θ = p1 * xj-1 + p2 * yj-1 + p3
22
获得 cosθ 和 sinθ 确定旋转矩阵R各元素的值
"cos_t" = cosθ
"sin_t" = sinθ
23
产生新向量 rj = aRrj-1 + c
xj = a * ("cos_t" * xj-1 - "sin_t" * yj-1) + c_x ;
yj = a * ("sin_t" * xj-1 + "cos_t" * yj-1) + c_y ;
24

图32

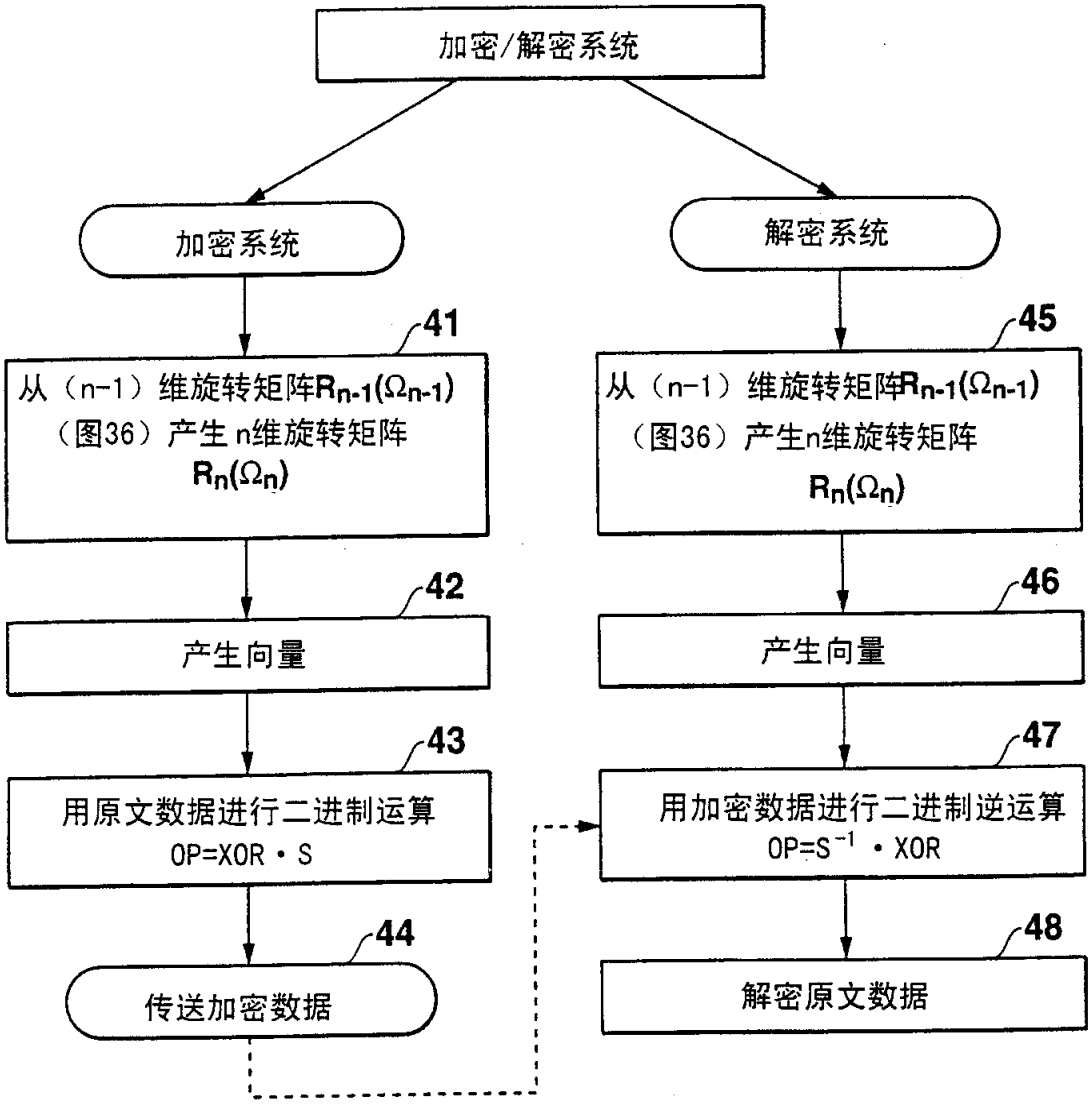

加密/解密系统
加密系统
解密系统
41
从（n-1）维旋转矩阵$R_{n-1}(\Omega_{n-1})$
（图36）产生 n维旋转矩阵
$R_n(\Omega_n)$
42
产生向量
43
用原文数据进行二进制运算
OP=XOR · S
44
传送加密数据
45
从（n-1）维旋转矩阵$R_{n-1}(\Omega_{n-1})$
（图36）产生n维旋转矩阵
$R_n(\Omega_n)$
46
产生向量
47
用加密数据进行二进制逆运算
$OP=S^{-1}$ · XOR
48
解密原文数据

图33

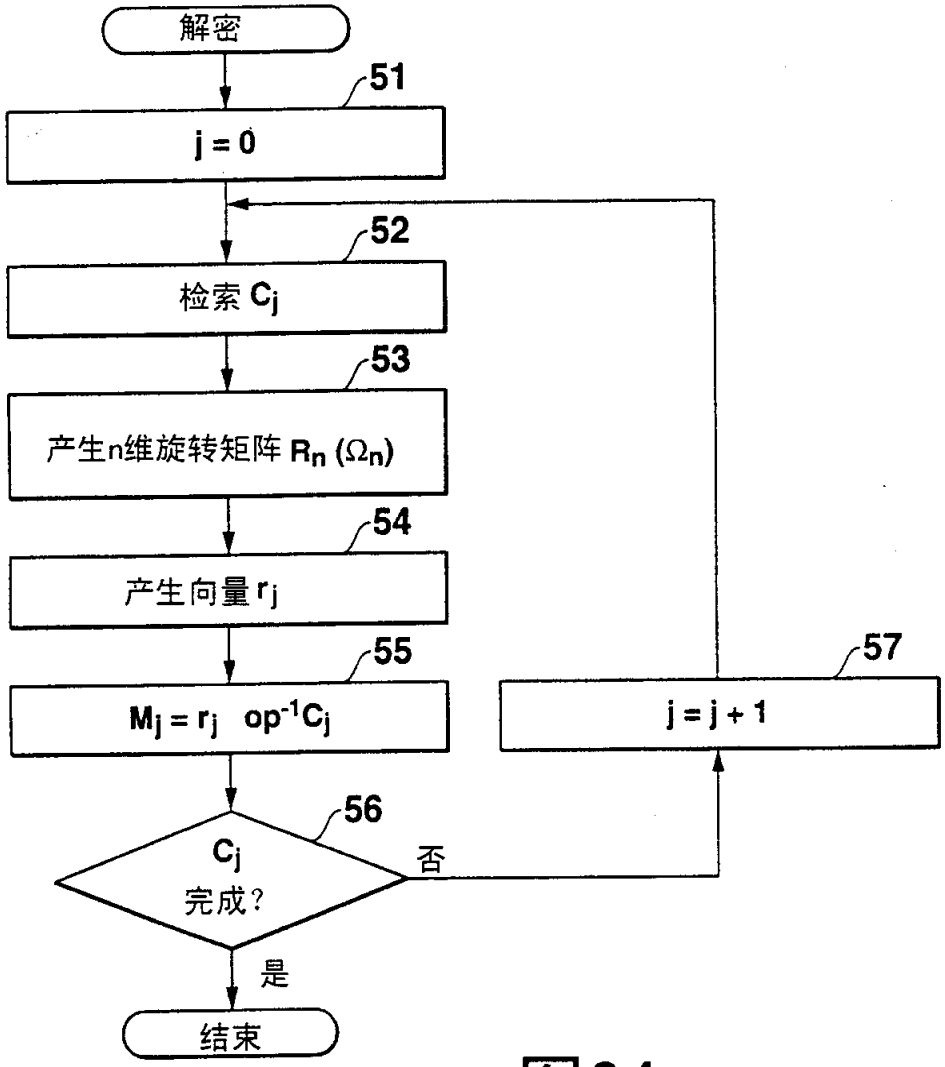

解密
51
j = 0
52
检索 Cj
53
产生n维旋转矩阵 Rn (Ωn)
54
产生向量 rj
55
Mj = rj op-1Cj
56
Cj
完成?
否
是
结束
57
j = j + 1

图34

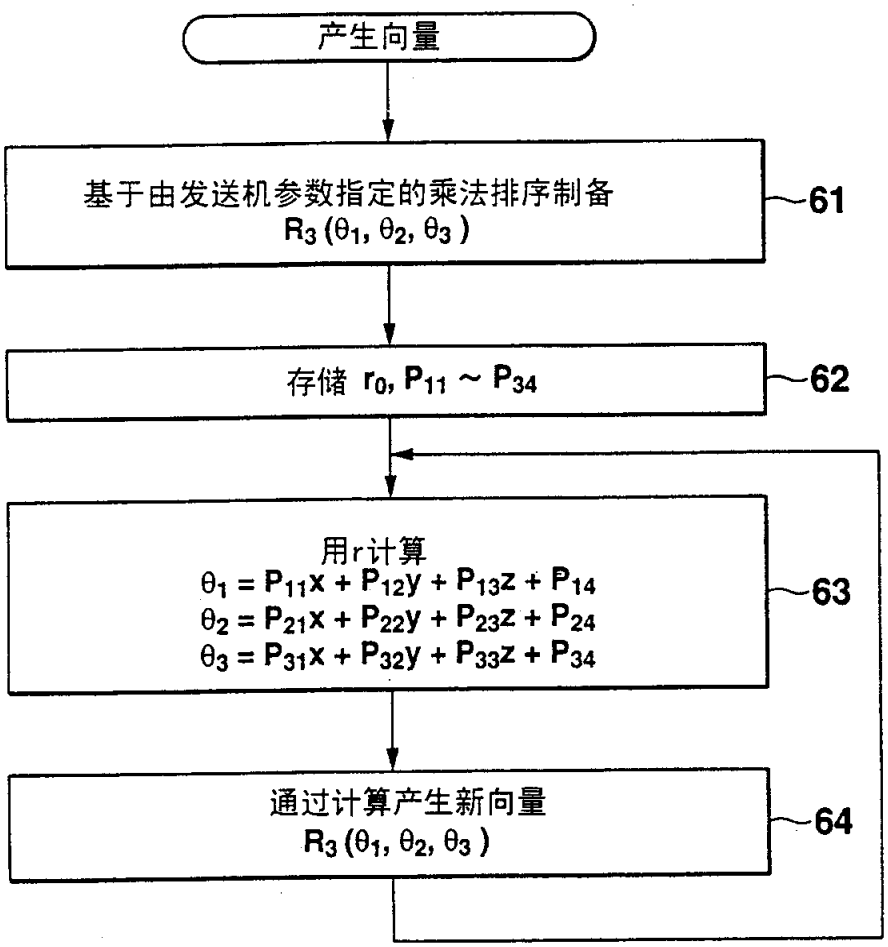

产生向量
基于由发送机参数指定的乘法排序制备
$R_3(\theta_1, \theta_2, \theta_3)$
61
存储 r_0, $P_{11} \sim P_{34}$
62
用r计算
$\theta_1 = P_{11}x + P_{12}y + P_{13}z + P_{14}$
$\theta_2 = P_{21}x + P_{22}y + P_{23}z + P_{24}$
$\theta_3 = P_{31}x + P_{32}y + P_{33}z + P_{34}$
63
通过计算产生新向量
$R_3(\theta_1, \theta_2, \theta_3)$
64

图35

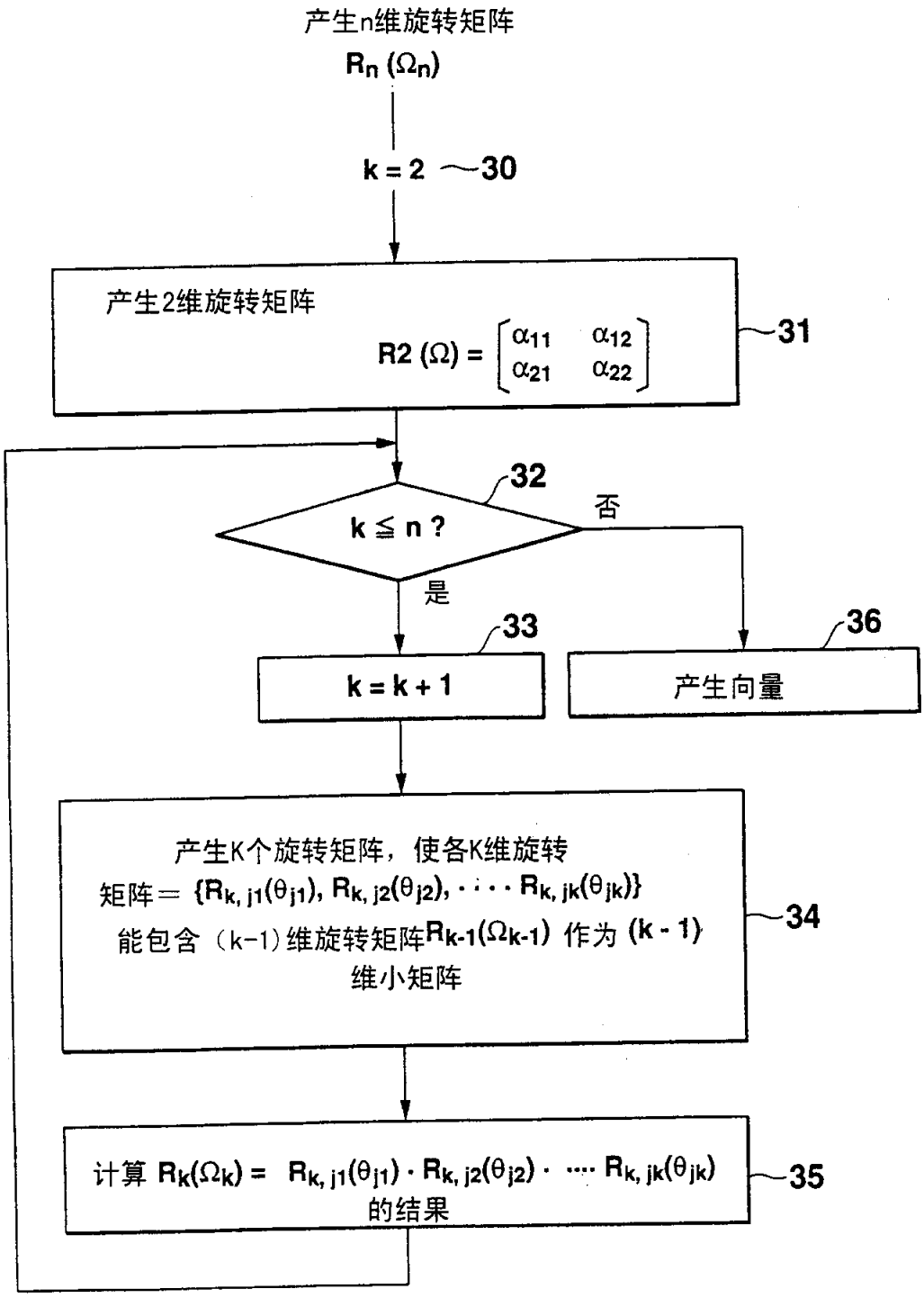

产生n维旋转矩阵
$R_n(\Omega_n)$
k = 2
30
产生2维旋转矩阵
$R2(\Omega) = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$
31
32
k ≦ n ?
否
是
33
k = k + 1
36
产生向量
产生K个旋转矩阵，使各K维旋转矩阵＝ $\{R_{k,j1}(\theta_{j1}), R_{k,j2}(\theta_{j2}), \cdots R_{k,jk}(\theta_{jk})\}$ 能包含（k−1）维旋转矩阵 $R_{k-1}(\Omega_{k-1})$ 作为 (k - 1) 维小矩阵
34
计算 $R_k(\Omega_k) = R_{k,j1}(\theta_{j1}) \cdot R_{k,j2}(\theta_{j2}) \cdot \cdots R_{k,jk}(\theta_{jk})$ 的结果
35

图36

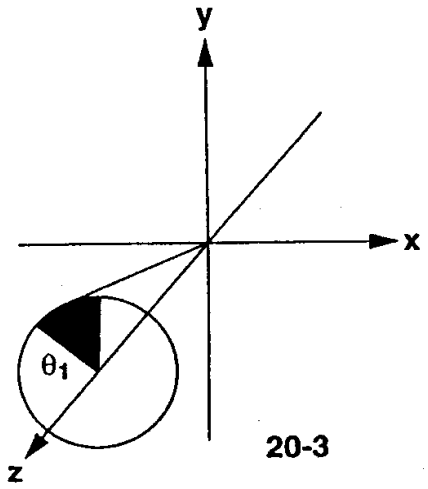


图37A

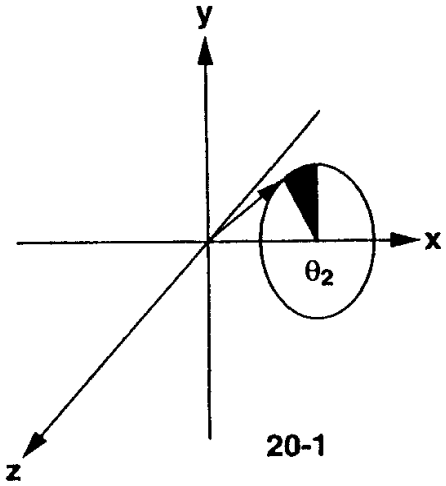


图37B

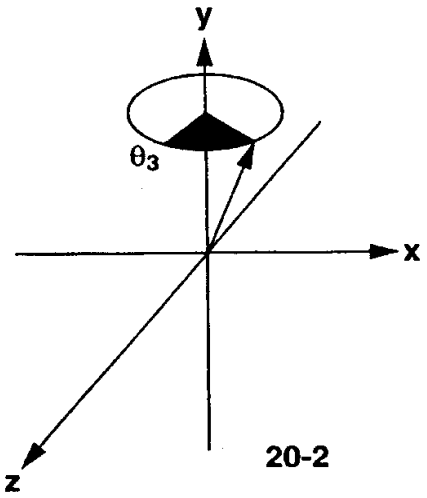


图37C