[19]中华人民共和国国家知识产权局

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

[12]发明专利说明书

[21] ZL 专利号 94113492.X

[45]授权公告日 2001 年 4 月 25 日

[11]授权公告号 CN 1065055C

[22]申请日 1994.12.28 [24]颁证日 2001.2.10
[21]申请号 94113492.X
[30]优先权
[32]1993.12.30 [33]FR [31]9315879
[73]专利权人 雅克·斯藤
地址 法国巴黎
[72]发明人 雅克·斯藤
审查员 孙继泉

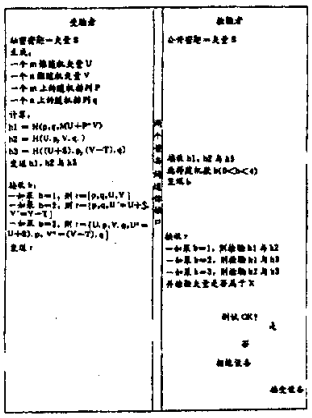
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 姜 华

权利要求书 5 页 说明书 14 页 附图页数 2 页

[54]发明名称 用一个检验者鉴别至少一个受验者的方法

[57]摘要

本发明涉及用一个检验者去鉴别至少一个受验者的一种方法,该鉴别方法基于 公开与秘密密匙密码技术,并利用零认识协议。此外,本协议是通过求解约束线 性方程组问题建立的。本发明可用于密码技术。



ISSN1008-4274

权 利 要 求 书

1、一种用于检验者根据使用秘密与公开密匙的密码技术 去鉴别至少一个受验者的方法，本鉴定方法用一种零认识协议达到，其中的公开密钥是应用约束线性方程组建立的。

2、按照权利要求1所述的方法，包括下述步骤：

①为了启动一次受验者与检验者之间的对话，建立一个秘密密匙，它包含至少一个n 维的其坐标选自一个固定集合X的矢量S；以及建立一个公开密匙，它包括含一个m×n 维的其系数为随机选自0至d-1的整数值的矩阵M，其中d 为接近一个数c的平方的一个素数；以及包含至少一个矢量P，使P=g(M(S))，其中g为一个由一集合X与整数(1，2，…d-1) 集合的子群G所定义的函数，并且g将G的元素g(x)与矢量P 的各坐标x相关联，使得x被唯一地描述成g(x)与X的元素k(x)的积；

②受验者接收由检验者生成的一个或多个随机数，然后向检验者返回一个提交，该提交是通过将一个密码散列函数作用在随S、M与该随机数而变的参数上而得出的；

③依据由检验者选择的随机数，检验者用所接收的值

与公开密匙，检验该提交是否正确。

3、按照权利要求2所述的方法，其中重复这些步骤若干遍，以提供较高的安全级别。

4、按照权利要求2所述的方法，其中集合X由c个元素构成，使得从1至d-1 的所有整数都能以唯一的方式被定义为G的一个元素与X的一个元素的积。

5、按照权利要求2所述的方法，其中的随机元素是用分别两个为m与n维的由0至d-1的整数组成的矢量，以及用两个分别为m与n个元素的排列p与q构成的。

6、按照权利要求2所述的方法，其中m=n。

7、按照权利要求2所述的方法，其中d=257及n=20。

8、按照权利要求2所述的方法，其中在各鉴别对话开始时，受验者向检验者透露其身份和/ 或其签名的公开密匙。

9、按照权利要求2所述的方法，其中，在受验者与检验者之间建立了对话并选定了随机元素之后：

①受验者计算通过一个散列函数H生成的提交h1与h2，并将它们发送至检验者：

$h1=H(p, q, MU+P^{*}V)$

$h2=H(U. p, V \cdot q)$

其中P*V指示与d同余的矢量P与V的分量的逐项积；

②检验者从0至d-1中随机选择一个数a 并将它发送给受验者;

③受验者计算下列矢量并将它们发送给检验者:

Y= (aS+U) . p

Z= (aT-V) . q

其中T为矢量k (M (S));

④ 检验者随机选择一位“b”，其中b=0或1，并将它发送给受验者;

⑤受验者返回一个如下定义的答复r:

- 如果b=0，则答复r由值p与q构成，
- 如果b=1，则答复r由矢量U' =S. p及V' =T. q构成;

⑥检验者接收答复r，并进行如下步骤:

- 如果b=0，则它从接收到的元素 (p，q) 中计算矢量Y'与Z'，使 (Y') . p=Y及 (Z') . q=Z，然后计算矢量M (Y') -P*Z'，如果答复是正确的，应使:

h1=H (p，q，M (Y') -P*Z') ;

- 如果b= 1，则检验者从接收到的元素中计算矢量Y -aU' 及aV' -Z，如果答复是正确的，应使:

h2=H (Y-aU' , aV' -Z)

并且检验者还检验矢量U' 与V' 中是否只包含X的元素。

１０、按照权利要求２所述的方法，其中，在建立了

受验者与检验者之间的对话，并且选定了随机元素之后：

①受验者计算通过一个散列函数H生成的提交h1、 h2与h3，并将它们发送给检验者：

h1=H(p, q, MU+P*V)

h2=H(U. p, V, q)

h3=H((U+S). p, (V-T). q)

其中P*V指定 与d同余的矢量P与V的分量的逐项积，而T则为矢量k(M(S))，它能被受验者作为S的一个函数计算出来，或存储在受验者存储器的一个物理上不可访问的部分中；

②检验者随机选择一个数“b”，使0〈b〈4，并将其发送给受验者；

③受验者返回一个如下定义的答复r：

- 如果b=1，则r由值p, q, U与V构成；
- 如果b=2，则r由值p, q及矢量U′=(U+S)与V′=(V-T)构成；
- 如果b=3，则r由值矢量U. p, V. q, U″=(U+S). p与 V″=(V-T). q构成；

④检验者接收答复r，并进行如下步骤：

·如果b=1，则它从所接收的元素(p, q, U与V)中计算 MU+P*V, U. p与V. q的值，如果答复是正确的，它们应使：

h1=H(p, q, MU+P*V)

h2=H(U. p, V, q);

· 如果b=2, 它从所接收的元素(p, q与矢量U'及V')中计算MU'+P V', U'. p与V' q的值, 如果答复是正确的, 它们应使:

h1=H(p, q, MU'+P*V')

h3=H(U'. p, V', q);

· 如果b=3, 它检验下式是否成立:

h2=H(U. p. V. q)

h3=H(U", V");

并且检验者还计算两个矢量U"-U. p及V"-V. q, 并检验它们是否 只由X的元素构成。

11、按照权利要求8所述的方法，其中鉴别操作的步骤被重复t遍，在此，t随所需的安全级别而增加， 只有当所有遍次的测试都成功时，检验者才证实受验者。

12、按照权利要求9所述的方法，其中矢量k(M(S))是由受验者把它作为S的函数计算的，或者是存储在受验者存储器的一个物理上不可访问的部分中。

说　明　书

用一个检验者鉴别至少一个受验者的方法

本发明涉及用一台检验设备去鉴别至少一台识别设备的一种方法，本鉴别方法利用一种基于约束线性方程组(CLE)问题的零认识的协议。

CLE问题在于找出一些值，这些值满足一定数目的与某一素数d同余的线性方程组，此外，这些值又为一个规定集合X的成员。

本发明特别适用于所谓“受保护的”或“安全的”通信，其中两台设备，一台识别设备(通常称作受验者)与一台检验设备(通常的称作检验者)，在一条其安全没有保证的信道上交换数据。在这种情况中，互相识别的手段是必不可少的。换言之，在给予一位用户访问数据或服务之前，必须使一位检验者能够鉴别该用户的身份。在许多情况下都需要这种受保护的通信手段。这类例子有传输金融业务的银行计算机、自动提款机、收费电视解码器及公用电话等。

对于这些应用，常用的鉴别方案是基于秘密密匙加密

方法的。直到目前为止，这一直是可资利用的最简单的技术。在这些实例中，受验者（通常是一张潇洒卡（SMART-CARD））检验者（诸如读卡机、解码器或公用电话）共用同一个秘密密匙。其鉴别是用一种对称算法或一个单向运算函数完成的。

这些方法的缺点是双方（受验者与检验者）必须互相合作且对外保密。这一条件并不是永远可以验证的。例如，由于秘密密匙是在通信线路的两端，即在受验者与检验者之中存在的，因此伪造者可以购置其检验设备并分析它，以了解其内部操作并随后制造高性能的设备。

众所周知，迄今为止的用于克服已有传统方法缺点的方法中，零认识协议能提供最高的安全级。这些零认识协议的功能性特征在于下述事实：即使与检验者进行无数笔交易且对这一检验者本身进行全面分析，也不足以复制该设备。在以下Fiat等人的名义申请的美国专利4748668 及以Shamir的名义申请的美国专利4932056中，值得注意地公布了零认识证明的描述。在后一专利中描述了一种基于所谓置换核心问题的称为“PKP”的鉴别方案。

本发明人研制了一种基于出错位组译码问题的新鉴别方案。这一问题在由Jacgues Stern 在CRYPTO93会议上提出的名为“基于出错位组译码的一种新鉴别方案”的论文

之中描述（该会议的报告集将在“计算机科学演讲笔记”中发表）。上述各种方法的缺点是受验者与检验者之间的信息交换较慢。此外，用在这些方法中的公开或秘密密匙通常是用非常大的位数编码的，需要可观的处理能力与存储器容量。

因此，本发明之目的在于提出一种使检验者能快速鉴别受验者并能采用中等大小的公开与秘密密匙的新鉴别方法，来克服上述缺点。

本发明之目的还在于采用一种根据秘密与公开密匙的密码技术的、由一个检验者鉴别至少一个受验者的方法，这一鉴别方法是用零认识协议完成的，其中的公开密匙是使用约束线性方程组建立的。这一方法最好包括下述步骤：

————为了启动受验者与检验者之间的对话，要建立一个秘密密匙，该秘密密匙由至少一个其坐标选自一固定集合$\mathbf{X}$的n维矢量$\mathbf{S}$构成；以及建立一个公开密匙，该公开密匙包括一个其系数随机地选自0至d-1整数值的m×n维矩阵m，其中d为接近一个数C的平方的素数；以及包括至少一个矢量P，使P= g(M(S))，其中g为一个由集合X 及整数集合(1，2，…，d－1)的子群G所定义的函数，并且该函数将G的元素g(x)与矢量P的各坐标x联系起来，使得x 被唯一地描述为g(x)与X的元素k(x)的积；

————受验者接收由检验者生成的一或多个随机数，然后将一个密码散列函数作用在是S、M与这些随机数的函数的参数上，把用这种方法得出的提交(commitment)返加给检证者；

————根据检验者所选择的随机数，检验者用接收的值与公开密匙检验该提交是否正确；

————根据所需的安全级，重复上述操作若干次。

在上述鉴别方案中，我们都使用一个所有用户公用的但随机地构造的m×n矩阵m。每一位用户收到一个其坐标选自一个固定集合X的n位字的秘密密匙S。这一集合X中包含c个元素，使得从1至d-1的所有整数都能被唯一地描述成G的一个元素与X的一个元素的积。在该情况下，该系统计算公开密匙P，使P=g（M(S)）。

此外，该鉴别过程主要基于提交(commitment)的技术概念，如果U是二进制元素的一个序列，则U的提交是通过一个给定的密码散列函数生成的U的象。该提交将被用作一个单向函数，换言之，它是通过公布一个用以建立它的原始序列而公开的。散列函数本身可用诸如R. Rivest在CRYPTO90会议上所描述的“MD4”法得出(CPYPTO90报告集，计算机科学演讲笔记集，303-311页)。我们也可使用按照名为“MD5”的方法这一方法的，或者美国标准SHA(安

全散列标准，联邦信息处理标准刊物，1992年10月30日提出）的变形。最后，也可以采用诸如DES（数据加密标准）的加密算法来代替散列函数，其中待散列的报文扮演密匙和/或要编码的明文的角色。但是我们建议选代这种散列，使散列的压缩结果好具有１２８位。

受验者也采用一个随机排列发生器来置换二进制矢量。这种发生器可由一个数字化的白噪声源制成。例如由所谓的“肘弯”区中的一个反向极化的二极管制成，也可利用Gunter的美国专利4、817、147、或Aragon的4、649、419中所描述的软件方法来制成。

按照以本发明为基础的鉴别过程的第一实施例，在全部各种过程分有的第一步骤中，受验者均将其身份和/或签有其名的公开密匙透露给检验者，然后：

————在随机选取两个分别为m与n维并由从0 至d-1的整数构成的矢量U与V及两个分别为m与n 个元素的排列p与q之后，受验者计算那些通过散列函数H生成的提交h1、h2与h3，并将它们发送给检验者：

h1=H(p, q, MU+P*V)

h2=H(U. p, V · q)

h3=H ((U+S). p, (V-T). q)

其中P*V表示与d同余的矢量P与V 的分量的逐项积；

而T则为矢量K（M(S)），它能被受验者作为S的一个函数计算出来，或者存储在该设备的存储器的一个物理上不可访问的部分中。

————检验者随机选择一个数字“b”，使0〈b〈4，并将它发送给受验者；

————受验者随即返回一个如下定义的答复r：

- 如果b=1，则r由值p，q，U与V构成；
- 如果b=2，则r由p，q，及矢量U′ =(U+S)与V′ =(V-T)构成；
- 如果b=3，则r由矢量U. p，V. q， U″ =(U+S) . p及V″ =(V-T) . q构成；

————检验者接收答复r，并进行如下步骤：

- 如果b=1，它便从接收到的元素（p，q，U与 V）中计算值MU+ P*V与V. p，如果答复正确的话，它们必定使：

h1=H(p，q，MU+P*V)

h2=H(U. p，V. q)

- 如果b=2，它便从接收到的元素（p，q，及矢量U′与V′）中计算值MU′+P*V′，U′. p与V′. g，如果答复正确的话，它们必定使：

h1=H(p，q，MU′+P*V)

h3=H(U′. p，V′. q)；

如果b=3，它便验证下式是否成立：

h2=H(U. p, V. q)

h3=H(U", V")

并且检验者还计算两个矢量U"-U. p及V"-V. q，并检验它们是否只由X的元素组成。

在按照本发明的鉴别过程的另一个优选实施例中，在所有各种过程公有的第一步骤中，受验者将其身份和/或其签名的公开密匙透露给检验者，然后：

——在随机选择两个分别为m与n维并由从o至d-1的整数构成的矢量U与V，及两个分别为m与n个元素的排列之后，受验者计算那些通过散列函数H生成的提交h1与h2，并将它们发送给检验者：

h1=H(p, q, MU+P*V)

h2=H(U. p. V. q)

其中P*V表示与d同余的矢量P与V的分量的逐项积；

————检验者从o至d-1中随机选择一个数"a"，并将其发送给受验者；

————然后，受验者计算下列矢量，并将它们发送给检验者：

$Y = (aS+U) \cdot p$

$Z = (aT-V) \cdot q$

其中T为矢量k(M(S))，受验者能将它作为S的函数计算

出来，或将它存储在该设备的存储器的一个物理上不能访问部分中。

————检验者随机选择一位"b"(=o或1)，并将它送至受验者：

————然后，受验者返回一个如下定义的答复r：

- 如果b=o，则r由值p与q构成，
- 如果b=1，则r由矢量U'=S.p与V'=Tq构成；

————检验者接收答复r并进行如下步骤：

- 如果b=0，它便从接收到的元素(p，q)中计算矢量Y'与Z'，使(Y)·p=Y及(Z')·q=Z，然后计算矢量M(Y')-P*Z'，如果答复是正确的，它必定使：

h1=H(p，q，M(Y')-P*Z')；

- 如果b=1，检验者计算矢量Y-aU'与aV'-Z，如果答复是正确的，它们必定使：h2=H(Y-aU'，aV'-Z)；

并且检验者还检验矢量U'与V'是否只包含X的元素。

在下面参照附图作为非限制性实例所取的两个较佳实施例的描述中，本发明的其它特征与优点将是显而易见的。

图1是说明按照本发明的鉴别过程的第一实施例的图；

图2是说明按照本发明的鉴别过程的第二实施例的图。

本发明涉及利用零认识协议的一种新的鉴别方案。在这种情况下，过程的安全性是基于约束线性组(CLE)问题

的。CLE问题在于找出n个值，这些值满足与一个素数d同余的一定数目的线性方程组，且又为一个规定集合X的成员。如果变量的数目是大的，则此问题非常难于用已知的计算方法求解。这里所描述的系统实际上对应于n+m个变量的m个方程的情况，其中m=n=20，这是极大地超出当今计算机能力的一种情况。

为了实现按照本发明的鉴别方案，有关当局选择并公布一个m×n维的矩阵M，其中最好m=n。这一矩阵包含一些从整数0至d-1中随机选出的系数，其中d通常为接近一个数c的平方的一个素数，最好d=257，即等于(16×16)+1。当局还选择n维矢量S的一个集合，其坐标是从一个集合X中随机选择的。该集合X是作为一个集合G的函数确定的，集合G是由与D同余的一个数的逐次幂级数构成的一个乘法群，这一集合被选择成使集合G中的元素个数为c。在这种情况下，便存在着一个也由c个元素构成的集合X，并且1与d-1之间的所有整数都可唯一地定义为，集合G中的一个元素与集合X中的一个元素的积。因此我们用g(u)来表示涉及在1与d-1之间的一个整数u的唯一分解的G的元素，并用k(u)表示X的对应元素。如果U是由1至d-1的整数组成的一个矢量，则g(u)是通过G由U的坐标的映象构成的，而k(u)也是类似地定义的。

将以这一方法所确定的秘密密匙分配给各受验者。此外，公布由矢量P=g(M(S))构成的所有公开密匙。在本发明的范围内，这一公开密匙与秘密密匙一样。可利用一张G与X的元素的表，只用少数字节编码。这样，如果d=257并且m=n=20，我们就得到10字节的密匙，这是本发明超过其它已知的零认识协议的一个优点。

下面描述为按照本发明的鉴别方案所特有的两个实施例。

第一过程参照图1描述，其中示意性地示出为了执行鉴别而用在受验者与检验者之间的通信协议。诸如潇洒卡或电子钥匙之类形式的受验者必须是物理上不可访问的。例如，在潇洒卡的情况下，必须是不能读取其内存的。另一方面，对检验者的工作环境不能施加任何要求。再者，受验者在其非易失性存储器中有其秘密密匙S，这就是n维的矢量S及m×n维的矩阵M；而检验者在其非易失性存储器中有用矢量P构成的所有公开密匙，或者有足够的数据来鉴别一个签名密匙P是否已由一个授权的当局产生。当受验者愿意与检验者通信时，这两个设备执行下述协议：

————首先，受验者向检验者透露其身份与/或签有其名的密匙；检验者确认其身份和P相符合；

————接着，受验者随机选择两个分别为m与n维的由0至d-1的整数构成的矢量U与V，其中最好m=n；加上两个分别

为m与n个元素的随机排列p与q。然后，受验者计算下列提交并将它们送到检验者：

h1=H(p, q, MU+P*V)

h2=H(U. p, V. q)

h3=〔(U+S). p, (V-T). q〕

其中P*V指定与d同余的矢量P与V的分量的逐项积，而T为矢量k(M(S))；

————检验者选择一个随机数“b”，使0〈b〈4，并将它送至验者；

————受验者将如下定义的一个答复 r送给检验者：

- 如果b=1，则r包含值p, q, U与V;
- 如果b=2，则r包含p, q, 及矢量U' = (U+S)与V' = (V-T)；
- 如果b=3，则r包含矢量U. p, V. q, V" = (U+S). p与V" = (V-T)；

————检验者接收答复r并进行如下步骤：

- 如果b=1，它从所接收的元素(p, q, U与V) 中计算MU+P*V, U · p与V.q的值；

如果答复是正确的，这些值应使：

h1=H(p, q, M+P*V)

h2=H(U. p, V, q)

- 如果b=2，它从所接收的元素(p, q, 与矢量U'及V')中计算MU' +P*V'，U' · p与V'. q的值，如果答复正确，它们应使：

h1=H(p. q, MU' +P*V')

h3=H(U' . p, V' . q)

• 如果b=3, 它验证下式是否成立:

h2=H(U. p, V. q)

h3=H(U", V")

并且检验者还计算两个矢量U"-U. p及V. q-S", 并检验它们是否只由X的元素构成。

如果上述测试全部成功，检验者便认为鉴别协议已成功地结束，并将一个控制信号发送到受保护系统的输入/输出接口，以启动一次业务；否则拒绝受验者

如果需要更高级别的安全性，检验者可重复上述步骤t遍。

在图1中概括了上述操作，其中左侧示出由受验者执行的操作，而右侧则为检验者执行的操作。

下面参照图2描述按照本发明的鉴别方案的另一个实施例。

第二实施例要求比前面一个作更多的计算，但更快地降低非法穿透该受保护系统的概率。这一实施例包含下述步骤，这些步骤概括在用与图1相同方式表示的图2中：

————首先，受验者向检验者透露其身份和/或其签名的密匙，象第一实施例一样；

————接着，受验者随机选择两个分别为m与n维（m可以等于n）的由0至d-1的整数构成的矢量U与V，加上两个分别为m与n个元素的随机排列p与q。然后受验者计算下述提交，并将它们送至检验者：

h1=H(p, q, MU+P*V)

h2=H(U. p, V. q)

其中P*V指定 与d同余的矢量P与 V的分量的逐项积，并且H为一个加密散列函数。

————检验者从0至d-1中选择一个随机数“a”，并将其送给受验者。

————受验者计算下列矢量，并将它们送至检验者：

Y=(aS+U). p

Z=(aT-V). q

其中T为矢量k(M(S))，它能被受验者作为S的一个函数计算出来，或者存储在该设备的存储器的一个物理上不可访问的部分中；

————检验者随机选择一位"b"(=o, 1)，并将其送至受验者；

————受验者返回如下定义的一个答复r：

- 如果b=o，则r包含值p与q，
- 如果b=1，则r包含矢量U'=S. p与V'=Tq；

———检验者接收答复r，并进行如下步骤：

• 如果b=o，它从所接收的元素(p. q) 中计算矢量Y'与Z'，使(Y')．p=Y及(Z')．q=Z，然后计算矢量M(Y')-ρ*Z'，如果答复正确，则矢量应使：

$$h1=H(p, q, M(Y')-\rho^{*}Z')$$

• 如果b=1，检验者计算矢量Y-aU'及aV'-Z，如果答复正确，则该两个矢量应使：

$$h2=H(Y-aU', aV'-Z)$$

并且检验者还检验矢量U'与V'，是否只包含X的元素。

如果关于b的测试是成功的，检验者便认为已成功地结束鉴别协议，并将一个控制信号送至受保护系统的输入/输出接口，以启动一次业务；否则拒绝受验者。

为了提高安全级别，受验者与检验者可重复上述步骤t遍，在这样的情况下，只有当所有遍数的测试都成功时才认为鉴别协议是成功的。最好的选择t使o<t<60。对于上述第一与第二实施例，值t＝35与t=20分别在许多应用中提供满意的安全级别。

上述两个实施例不是限制性的，它们可用若干方法修正而仍保持在本发明的范围中。

说　明　书　附　图

图 1

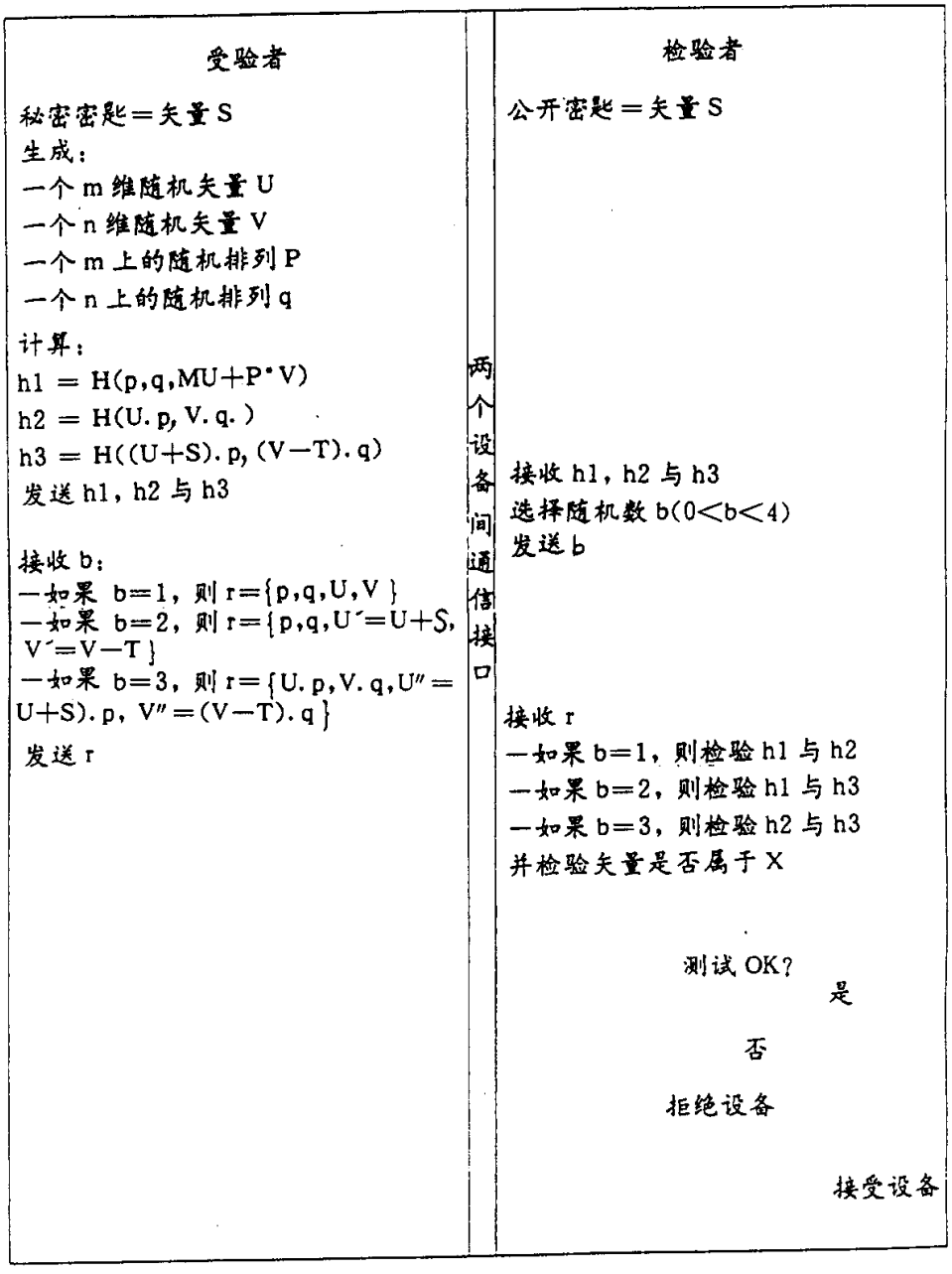

受验者
秘密密匙＝矢量 S
生成：
一个 m 维随机矢量 U
一个 n 维随机矢量 V
一个 m 上的随机排列 P
一个 n 上的随机排列 q
计算：
h1 ＝ H(p,q,MU＋P*V)
h2 ＝ H(U.p, V.q.)
h3 ＝ H((U＋S).p, (V－T).q)
发送 h1，h2 与 h3
接收 b：
－如果 b＝1，则 r＝{p,q,U,V}
－如果 b＝2，则 r＝{p,q,U′＝U＋S, V′＝V－T}
－如果 b＝3，则 r＝{U.p,V.q,U″＝U＋S).p, V″＝(V－T).q}
发送 r
两个设备间通信接口
检验者
公开密匙＝矢量 S
接收 h1，h2 与 h3
选择随机数 b(0＜b＜4)
发送 b
接收 r
－如果 b＝1，则检验 h1 与 h2
－如果 b＝2，则检验 h1 与 h3
－如果 b＝3，则检验 h2 与 h3
并检验矢量是否属于 X
测试 OK?
是
否
拒绝设备
接受设备

图 2

受验者	两个设备间的通信接口	检验者
秘密密匙＝矢量 S		公开密匙＝矢量 S
生成： 一个 m 维随机矢量 U 一个 n 维随机矢量 V 一个 m 上的随机排列 p 一个 n 上的随机排列 q		
计算： h1 ＝ H(p,q,MU＋P*V) h2 ＝ H(U.p, V.q)		
发送 h1，h2 与 h3		接收 h1 与 h2 选择随机数 a(0＜a＜d－1) 发送 a
接收 a 计算： Y ＝ (aS＋U).p Z ＝ (aT －V).q T ＝ k(M(S)) 发送 Y 与 Z		接收 Y 与 Z 选择随机位 b(b＝0,1) 发送 b
接收 b： —如果 b＝0，则 r＝{p,q} —如果 b＝1，则 r＝{U´＝S.p,} V´＝T.q} 发送 r		接收 r： —如果 b＝0，则检验 h1 —如果 b＝1，则检验 h2 并检验矢量是否属于 X
		测试 OK？ 是： 否 拒绝设备
		接受设备