[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04L 9/32

[12]发明专利申请公开说明书

[21]申请号 99812286.6

[43]公开日 2001年11月21日

[11]公开号 CN 1323478A

[22]申请日 1999.8.16 [21]申请号 99812286.6
[30]优先权
[32]1998.8.17 [33]FR [31]98/10591
[86]国际申请 PCT/FR99/01995 1999.8.16
[87]国际公布 WO00/10287 法 2000.2.24
[85]进入国家阶段日期 2001.4.17
[71]申请人 格姆普拉斯公司
地址 法国基米诺斯
[72]发明人 L·鲁索
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 王 勇 李亚非

权利要求书2页 说明书5页 附图页数1页

[54]发明名称 用对称算法验证的方法和设备

[57]摘要

本发明涉及用对称算法验证的方法和系统,其主要特征在于,为两方的各自相互验证,执行一个对称之为K'的可变密钥的密码计算。所说的方法的主要步骤如下:a)拥有保密密钥K的A方发送一个随机数R_1到B方,后者也拥有相同的保密密钥K;b)B方选择一个随机数R_2,并根据如下公式计算数K',它也是一个保密密钥:$K' = R_2 xor K$, xor等价于"异或"的数学运算;c)然后B利用对称加密算法ALG计算由如下公式得到的一个结果r: $r = ALG[K'](R_1)$;d)所说的B方然后发送r和R_2给所说的A方;e)所说的A方利用相同的对称加密算法ALG采用如下公式计算K'和r': $K' = R_2 xor K$和$r' = ALG[K'](R_1)$;f)如果r等于r',则所说的B方被所说的A方验证。

ISSN1008-4274

权　利　要　求　书

1. 在拥有相同的保密密钥 K 的两个实体或两方 A 和 B 之间用对称加密算法验证的方法，其特征在于它执行如下的验证步骤:

a) 拥有保密密钥 K 的 A 方发送一个随机值或随机选取的数 R_1 到 B 方，后者也拥有相同的保密密钥 K;

b) B 方选择一个随机数 R_2 并采用如下公式计算数 K'，它也是一个保密密钥:

$K'=R_2$ xor K，xor 等价于数学的“异或”;

c) 其次，B 利用对称加密算法 ALG 计算由如下公式得到的一个结果 r:

$r=ALG[K'](R_1)$

d) 所说的 B 方然后发送 r 和 R_2 给所说的 A 方;

e) 所说的 A 方利用相同的对称加密算法 ALG 采用如下公式计算 K' 和 r':

$K'=R_2$ xor K

和

$r'=ALG[K'](R_1)$。

f) 如果 r 等于 r'，则所说的 B 方被所说的 A 方验证。

2. 按照权利要求 1 的方法，其特征在于密钥 K 利用下面的公式被分解成一组 n 个子密钥 k_i，i 是子密钥的下标:

$K = k_i$ xor k_2 xor…xor kn。

3. 按照权利要求 1 或 2 的方法，其特征在于它包括以如下公式来计算 K' 的系统，K' 依子密钥 K_i 使用的次序成为随机的，而 i 是子密钥下标:

$K' = R_2$ xor k_1 xor…xor kn。

4. 按照权利要求 3 的方法，其特征在于保密密钥 K' 利用包括一个初始化阶段和一组循环的算法被计算。

5. 按照权利要求 4 的方法，其特征在于初始化阶段包括;

—第一个表 k，或 k[]，包含 n 个子密钥 k_i，和

—第二个表，称之为 to-do，或 to-do[]，包含 n 个布尔值，每个布尔值包含称为“True”或“T”的真值，

以及其特征在于表 k[]和 to-do[]包含相同数目的 n 个元素，其

代表 n 个子密钥 k_i 和 n 个布尔值。

6. 按照权利要求 4 的方法，其特征在于算法循环包括如下步骤:

a) 第一个步骤由下列事实组成，即只要表 to-do[]中仍有一个元素的值为“T”，则在 1 和 n 之间的随机数 i 被选择;

b) 第二个步骤包括测试在表 to-do[]中元素 i 具有值“T”;

c) 如果第二个步骤的结果是真，则第三个步骤包括两个运算:

—首先，将 K'和表 k[]的第 i 个元素之间数学“异或”的结果分配给变量 K'，其是按如下公式计算:

K'=K' xor k[i]

—第二是将下文和图中称之为“F”的值“False”分配给表 to-do[]中下标 i 的元素: to-do[i]=“F”。

7. 按照权利要求 4 的方法，其特征在于算法循环由下列步骤组成:

a) 第一个步骤由下列事实组成，即只要表 to-do[]中仍有一个元素的值为“T”，则在 1 和 n 之间的随机数 i 被选择;

b) 第二个步骤包括测试在表 to-do[]中元素 i 具有值“T”;

c) 如果第二个步骤的结果是假，则计算系统返回到第一个步骤。

8. 在拥有相同的保密密钥 K 的两个实体或两方 A 和 B 之间用对称加密算法验证的一个系统，其特征在于它实现按照权利要求 1 至 7 的任一个的验证方法。

01.04.17

说　明　书

用对称算法验证的方法和设备

本发明涉及用对称算法验证的方法，其具有的主要特征在于，对于通常称之为A和B的两方的各自相互验证，执行一个对可变密钥（称之为K'）的密码计算。

更精确地说，本发明涉及在称之为A和B且在数据交换情况下相互无关的两方的验证期间上面所引述的密码计算。这可以是在PC和服务器之间，在阅读器和服务器之间，在单片卡和单片卡读出器之间，举例来说，诸如一台在使用单片卡情况下的自动取款机，被称之为A，一个希望取钱的来到取款机旁的用户，被称之为B。

更具体地说，两方A和（或）B可以被当作是一个单片卡和（或）一个读出器。

专家知道，保密问题对取款机和单片卡类型的装置的正确运行是关系重大的。这些关注是继续和更有效的保护措施的主题，以使对此的攻击愈来愈难以得逞。

为了解释这个情况，在密码术的技术领域中，大家知道互相联系的两方被称为A和B。

在更多的技术和科学术语中，该方法由一定数目的步骤组成。

具体地说，拥有一个保密密钥K的A选择一个随机值R，或随机数，也称之为一个消息。

A发送这个随机值R至也拥有相同保密密钥K的B。

B利用对称加密算法ALG通过如下公式计算一个结果，称之为r:

r=ALG[K](R)。

r是用算法ALG和保密密钥K的消息R的加密的结果。称作ALG的算法是一个对称加密算法。这可以是DES（数据加密消息），三重DES，IDES等。

这个运算可以被执行，因为保密密钥对两方A和B是已知的，且只有A和B知道。

其次，B发送结果r到A。后者A然后利用如下公式计算结果r':

r'=ALG[K](R)。

如果数r等于结果r'，则B被验证。

B 被 A 的验证是以这种方式完成的。

然而，这个操作是不充分的，因为它对电流测量因而对可能的侵犯者的攻击是脆弱的。

一个攻击者，或侵犯者测量该片的电流消耗。根据所得到的曲线，他可以推断出管理中的信息和处理机所使用的数据。为了实施精密的测量，攻击者必须进行多次测量并筛选它们。

更确切地说，问题在于 r 的计算，也就是说在于公式：

r=ALG[K](R)。

这是因为电流测量在这个水平上易于实现，因此经由计算可以知道数据，特别是因为密钥 K 是常数。

为了获得一个中肯的测量，侵犯者必须执行多次测量并筛选它们，以便从中提取中肯的信息。因为使用相同的常数密钥 K，所以所有测量都使用相同的密钥 K，因此筛选的结果是密钥 K 特有的。

本发明提出一个第一个特性，其由一个简明的修改组成，该修改在作为本发明目的验证协议的 r'计算公式中进行。

拥有保密密钥 K 的 A 方发送一个随机值或随机选取的数 R_1 到 B 方。后者也拥有相同的保密密钥 K。

B 选择一个随机数 R_2，然后使用如下公式计算数 K'，它也是一个保密密钥：

$K'=R_2$ xor K，xor 是数学符号“异或”。

其次，B 计算由如下公式引起的一个结果 r：

$r=ALG[K'](R_1)$

B 然后发送 r 和 R_2 给 A。

后者利用相同的对称加密算法 ALG 采用如下公式计算 K'和 r'：

$K'=R_2$ xor K

和

$r'=ALG[K'](R_1)$。

假设 r 等于 r'，则 B 被 A 验证。

在此刻攻击的不可能性基于下面的事实，即因为 K'在每次验证时是变化的，计算 r 和 r'的电流消耗在每次执行验证时是不同的。

然而，K'的计算对攻击仍是脆弱，因为涉及电流消耗。因此，本发明提出一个第二个特性，其与上述的第一个特性无关，仅与 K'的计

算有关。

这是因为本发明使用一个与上述的验证系统无关和（或）相关的加密系统。

它由K'的计算组成，K'是随机产生的。

为此目的，保密密钥K利用下面的公式被分解成一组n个子密钥k_i，i是子密钥的下标：

$K = k_i \text{ xor } k_2 \text{ xor} \cdots \text{xor } kn$。

因此，K'的计算以另一个公式表述如存在那样是可能的：

$K' = R_2 \text{ xor } k_1 \text{ xor} \cdots \text{xor } kn$。

因为运算符xor的置换性质，所以有可能改变计算的次序，以便在每次验证时获得一个不同的计算。

为了建立k和k'之间的联系，所采用的算法包括一个初始化阶段和一个循环子集。

算法的初始化必须首先概括地说明，然后通过解释一个具体情况，最后可互换到普遍的情况。

下面的陈述解释初始化。

一般地说，第一个表k（在下面的描述中称之为k[]）被采用；这个表包含n个子密钥k_i的值。

称之为to-do的第二个表（下文称之为to-do[]）包含n个布尔值。每个布尔值包含真值，下面和在图2中称之为“True”或“T”。表k[]和to-do[]包含相同数目的n个元素，代表n个子密钥k_i和n个布尔值。

值R_2被分配给K'，或更确切地说$K' = R_2$。

算法的循环在下面描述并在图1中绘出：

第一个步骤，即步骤a由如下事实组成，即只要表to-do[]中仍有一个元素的值为“T”，则在1和n之间的随机数i被选择。

随后的步骤，步骤b，测试在表to-do[]中的元素i与在下文和图中称之为“T”的值的等同性。

如果等同性测试为真，则执行两个运算：

一首先，步骤c是将K'和表k[]的第i个元素之间的数学“异或”的结果分配给变量K'，事实上它是下列公式的计算：

K'=K' xor k[i]

一第二，步骤 d 是将下文和图中称之为“F”的值“False”分配到表 to-do[]中下标 i 的元素：to-do[i]=“F”。

如果步骤 b 的等同性测试为假，则计算系统返回到第一个步骤，即步骤 a。

这个算法不是恒定时间，因为有可能执行比子密钥 k_i 要多的循环。

本发明也涉及在拥有相同的保密密钥 K 的两个实体或两方 A 和 B 之间用对称加密算法的一个验证系统，其实现上述的方法。

本发明现在将用一个确切例子的实施例来描述，如仅描述二个循环的图 2 所示，其是子密钥数目 n 等于 2，n=2 的情况。

初始化与上述的一般情况仍相同；在图 2 中用附注 A 或 10 示出。

算法的循环被实施如下：

算法的两个计算是可能的。

不是将执行下面的运算：

$K'=R_2$ xor k_1 xor k_2;

就是将执行下面的运算：

$K'=R_2$ xor k_2 xor k_1;

因此，侵犯者不知道一开始将执行哪个计算，因此不能使用多次测量进行筛选。

在一次循环变换或第一次尝试中填入两个元素的概率是零，或者以更明白和可见的方式（参见图 2）来说，在一次尝试中在表 to-do[]的两个元素中投放值“F”的概率为零。因此，在一次循环中不可能获得两个相同的值“F”、“F”。

其次，在两个循环或两次尝试中在表 to-do[]的两个元素中投入值“F”的概率等于二分之一或 1/2。

这是因为在第一个循环时，随机数 i 等于 1（20）可 2（21），i=1 或 2，被选择；然后值“F”被放进表 to-do[]两个元素中的一个内；这个第一个循环在图 2 中标示为 B。

在第二个循环（参见图 2）时，随机数 i 等于 1 或 2，i=1 或 2，被选择；然后值“F”根据所选择的随机数被放进表 to-do[]两个元素中一个内；这个第二个循环在图 2 中标示为 C。

因此有两种已终止的情况（31，32），也就是说在两个元素中为

两个值“F”，和两个未终止的情况（30，33）；K'的计算没有被终止。获得这个结果的概率是二分之一。

此外，在第三个循环或尝试中填入两个元素的概率等于四分之一，或1/4（图2中未示出）。

这是因为随机数i等于1或2被选择；值“F”不是被投放到表to-do[]的第一个元素内就是投放到第二个元素内。

因此，象在第二个循环时一样，有两个已终止的情况，也就是说在两个元素中为两个值“F”，以及两个未终止的情况。K'的计算没有被终止。

更一般地说，在k次循环中填入两个元素的概率等于$1/2^{k-1}$。

知道为了发生于两个元素每个包含值“F”要执行的循环的平均值S是有利的。

为此，数学期望被计算并列出公式如下：

$$S=\sum_{i=2}^{n} i\times\frac{1}{2^{i-1}}$$

这个数学期望是概率的加权和。

经计算，它等于三。

因此结论为：S = 3。

K'的计算平均以三次循环来完成。

说 明 书 附 图

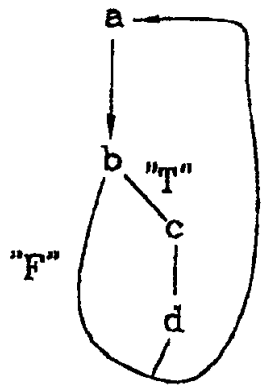

图 1

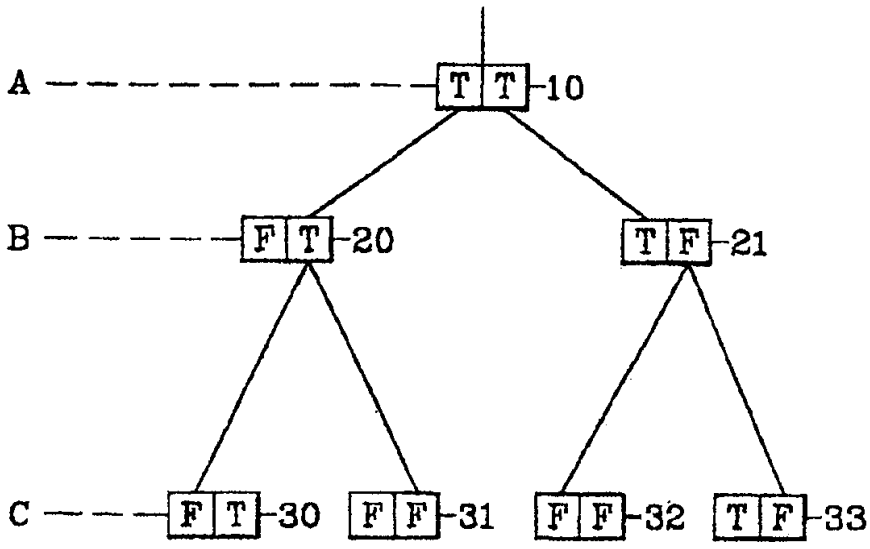

图 2