[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 00812293.8

[45] 授权公告日 2008 年 12 月 31 日

[11] 授权公告号 CN 100448193C

[22] 申请日 2000.8.24 [21] 申请号 00812293.8

[30] 优先权

[32] 1999.8.30 [33] CH [31] 1573/99

[32] 2000.4.3 [33] US [31] 60/194,171

[86] 国际申请 PCT/IB2000/001157 2000.8.24

[87] 国际公布 WO2001/017159 法 2001.3.8

[85] 进入国家阶段日期 2002.2.28

[73] 专利权人 纳格拉卡德股份有限公司

地址 瑞士舍索 - 苏尔 - 洛桑

[72] 发明人 马尔科·萨塞利

克里斯托弗·尼科拉斯

迈克尔·约汉·西尔

[56] 参考文献

US 5594797A 1997.1.14

审查员 江靖敬

[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 李德山

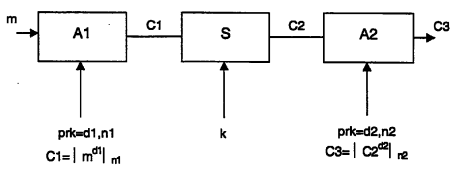
权利要求书 2 页 说明书 7 页 附图 2 页

[54] 发明名称

多模块加密方法

[57] 摘要

当用一个加密/解密模块时，存在着许多通过分析进入或离开模块的数据确定模块所用的一个密钥或多个密钥的方法。 为了解除这些方法的缺点，提出的多模块方法在于一旦上游的加密/解密模块已发出了其部分计算结果时，下游加密/解密模块就开始其加密/解密运算。



1. 利用至少三个串联的加密/解密模块的加密和解密方法，其特征在于中间和最后的加密/解密模块中的每一个模块在紧邻的前一个加密/解密模块结束加密/解密运算之前一旦已经可得到部分信息，就开始进行加密/解密运算。

2. 根据权利要求 1 的方法，其特征在于中间和最后的解密模块中的每一个模块一旦已经可从紧邻的前一个解密模块得到部分信息，就开始进行解密运算。

3. 根据权利要求 1 的方法，其特征在于中间和最后的加密模块中的每一个模块一旦已经可从紧邻的前一个加密模块得到部分信息，就开始进行加密运算。

4. 根据权利要求 1 到 3 之一的方法，其特征在于它用 3 个模块（A1，S，A2），中央模块（S）为使用秘密对称密钥（k）的类型。

5. 根据权利要求 4 的方法，其特征在于，对于加密来说的第 1 模块（A1）和最后模块（A2），以及对于解密来说的第 1 模块（A2）和最后模块（A1），为使用非对称密钥即一个专用密钥和一个公开密钥的 RSA 类型。

6. 根据权利要求 5 的方法，其特征在于所述两个模块（A1，A2）对于加密用所谓的专用密钥（d，n；d1，n1；d2，n2），对于解密用所谓的公开密钥（e，n；e1，n1；e2，n2）。

7. 根据权利要求 6 的方法，其特征在于所述两个模块（A1，A2）用相同的专用密钥（d，n）和公开密钥（e，n）组。

8. 根据权利要求 6 的方法，其特征在于所述两个模块（A1，A2）用不同的专用密钥（d1，n1；d2，n2）和公开密钥（e1，n1；e2，n2）组。

9. 根据权利要求 5 的方法，其特征在于当加密时，最后模块（A2）用所谓的公开密钥（e2，n2），当解密时，第 1 模块（A2）用所谓的专用密钥（d2，n2）。

10. 根据权利要求 1 到 3 之一的方法，其特征在于它用 3 个使用非

对称密钥的加密/解密模块（A1，A，A2）。

多模块加密方法

本发明涉及数据的加密或解密领域，特别是涉及在付费观看电视系统的框架内对未授权的人或设备保持不可访问的数据的加密或解密。在这种系统中，在保密环境中对数据进行加密，该环境提供相当大的计算能力并称为编码子系统。然后用已知的方法将数据发送给至少一个分散子系统，在该分散子系统中一般用 IRD（Integrated Receiver Decoder，综合接收机解码器）并在一张芯片卡的帮助下对数据进行解密。一个可能的非授权者能够不受限制地访问这个芯片卡和与芯片卡合作的分散子系统。

在一个加密/解密系统中将许多不同的加密/解密方法链接起来是已知的做法。在以下的述说中，用术语加密/解密表示用于一个较大的加密/解密系统中的一个特定的加密方法。

长时期来一直在设法从速度，占据的存储空间和保密性这样三个观点使这些系统的工作最佳化。这里将速度理解为意指对接收的数据进行解密所需的时间。

具有对称密钥的加密/解密系统是已知的。能够作为若干判据的函数对它们的固有的保密性进行估计。

第 1 个判据是物理保密性的判据，与通过析取某些成分，接着可以用其它成分替换它们的调查方法的难易有关。这些打算向非授权者通报加密/解密系统的工作性质和方式的替换成分被他/她以这样一种不能由系统其它部分探测的或尽可能不能探测的方式进行选择。

第 2 个判据是系统保密性的判据，在它的框架内攻击从物理观点来看不是直观的但是要求分析数学类型。典型地，这些攻击将由企图破译算法和加密码的具有高计算能力的计算机进行。

具有对称密钥的加密/解密的方法例如是称为 DES（Data Encryption Standard，数据加密标准）的系统。这些相对古老的方法现在只提供完

全相对的系统保密性和物理保密性。特别是因为这个原因，DES，它的密钥长度太短不能满足系统保密性的条件，正在越来越多地被新的加密/解密方法所替换或用较长的密钥。一般，这些具有对称密钥的方法要求包含加密圈的算法。

其它的攻击战略称为单功率分析和定时分析。在单功率分析中，我们利用一台用于对数据进行加密或解密的微处理机与一个电压源(一般为5伏）连接这样一个事实。当它空载时，有大小为i的固定的电流流过它。当它在工作时，瞬时值i不仅与输入数据而且与加密算法有关。单功率分析在于测量电流i作为时间的函数。可以从它推导出微处理机实施的算法类型。

以同样的方式，定时分析方法在于测量计算的持续时间作为提供给解密模块的样本的函数。这样，在提供的样本和用于计算结果的时间之间的关系使恢复解密模块秘密参数如密钥成为可能。例如在由 Paul Kocher， Cryptography Research， 870 Market St， Suite 1088， San Francisco，Ca-USA 公布的文件“Timing Attacks on Implememtations of Diffie-Hellman，RSA，DSS，and Other Systems”中描述了这样一种系统。

为了改善加密系统的保密性，已经提出了具有非对称密钥的算法，如所谓的 RAS（Rivest，Shamir and Adleman）系统。这些系统包含产生一对匹配密钥，其中一个是所谓的用于加密的公开密钥，而另一个是所谓的用于解密的专用密钥。这些算法显示出保密性，系统和物理保密性两者的高水平。另一方面，它们比传统的系统，特别是在加密阶段慢。

最近的攻击技术要求代表微分功率分析的所谓的 DPA 概念。这些方法的基础是在大量试验后可以证明的，关于在加密密钥的一个给定位置上存在一个 0 或一个 1 的推测。它们几乎是非破坏性的，这样使它们具有很大的不可探测性，并要求物理入侵成分和数学分析成分两者。它们的工作方式使我们想起探测油田的技术，在那里在地球表面上产生已知功率的爆炸，并在离开爆炸点的已知距离处放置耳机和探针，不需进行太多的挖掘，利用由该地表下面的沉积床的边界反射的冲击波，就能够关于地表下的地层学成分作出假设。在由 IBM T.J.watson Research

Center，Yorktown Heights，NY 的 Suresh Chari，Charanjit Jutla，Josyula R.Rao and Pankaj Rohatgi 于 1999 年 2 月 1 日公布的文件“A Cautionary Note Regarding Evaluation1of AES Candidates on Smart-Cards”的第 2.1 节中特别描述了 DPA 攻击。

必须阻止 DPA 攻击的要求迫使或者在输入信息中或者在加密/解密算法的输出上使用所谓的“白化”干扰系统。在上述的同一个文件的第 3.5 节中描述了白化技术。

然而，在付费观看的电视系统的分散子系统中计算能力受到限制的事实，对于上面描述的实施足够程度的链接，产生一个从来没有被令人满意地解决过的问题。

本发明的目的是使对抗如上面描述的现代调查方法的加密/解密方法变成可以利用的。

本发明的目的通过下述方法实现：利用至少三个串联的加密/解密模块的加密和解密方法，其特征在于中间和最后的加密/解密模块中的每一个模块在紧邻的前一个加密/解密模块结束加密/解密运算之前一旦部分信息已经可利用，就开始进行加密/解密运算。

本方法的特点在于这样一个事实，即中间模块不是当来自前面（或上游）模块的结果已经终止时开始工作，而是一旦已经可得到部分信息时就开始工作。所以，对于一位外部的观察者，对于这个模块不可能建立起输入或输出条件。

因为在与芯片卡合作的分散子系统中，这个芯片卡提供与编码子系统比较只是相对地受到限制的计算能力，发生解密，所以例如用一个当解密的最后步骤中工作得相对快的公开的非对称密钥是有益的。这一方面使在脱离过程中保持系统的不受破坏性的特征，另一方面使在编码子系统中在专用密钥的帮助下集中基本上与加密有关的计算能力成为可能。

我们已经发现由于链接或部分交错的两个相互时序地跟随的加密/解密方法的可能性提供额外的保密性。我们将链接或部分交错理解为意味着该过程在于当第 1 个加密/解密方法还没有结束它对数据的工作时，就开始第 2 个加密/解密方法对这些同样的数据的工作。这使得像它们是由

于第 1 模块的工作引起那样地并在受到第 2 模块的作用前掩蔽数据成为可能。

一当在第 1 模块的输出端计算得到的数据部分可用于由第 2 模块进行的处理时链接就能够立即开始。

本发明通过在一个加密/解密系统中将许多不同的加密/解密方法组合起来和可能通过将链接或部分交错与这些方法在其中相互跟随的序列结合起来，使保护不受上述攻击成为可能。

在本发明的一个特定的实施例中，加密/解密系统包含一个时序地使用三个算法的编码子系统:

a) 一个具有专用密钥 d1 的非对称算法 A1。这个算法 A1 在由消息 m 表示的明文数据上加上签字，这个操作通过在专业上一般由下列公式表示的数学操作传递第 1 个密报 c1 : c1=m 指数 d1，模 n1。在这个公式中，n1 形成非对称算法 A1 的公开密钥的一部分，模代表在该组相关整数内众所周知的数学的同余算子，d1 是算法 A1 的专用密钥。

b) 一个用秘密密钥 K 的对称算法 S。这个算法将密报 c1 变换成密报 c2。

c) 一个具有专用密钥 d2 的非对称算法 A2。这个算法 A2 用如上所述的下列公式表示的数学操作将密报 c2 变换成密报 c3 : c3=c2 指数 d2，模 n2，在这个公式中，n2 形成非对称算法 A2 的公开密钥的一部分，d2 是算法 A2 的专用密钥。

用本身已知的方法，密报 c3 离开编码子系统并到达分散子系统。在付费观看的电视系统的情形中，这可能同等地涉及视频数据或消息。

分散子系统以与上述相反的次序使用 3 个算法 A1′，S′和 A2′。这 3 个算法形成分布在编码子系统和分散子系统之间的 3 个加密/解密方法 A1-A1′，S-S′和 A2-A2′的一部分，并代表加密/解密系统。

d) 算法 A2′对 c3 实施恢复到 c2 数学操作，并表示为：c2=c3 指数 e2 模 n2。在这个公式中，由 e2 和 n2 构成的组是非对称算法 A2-A2′的公开密钥。

e) 对称算法 S′用秘密密钥 K 恢复密报 c1。

f) 具有公开密钥 e1，n1 的非对称算法 A1′通过实施下面表示的数学操作恢复 m: m=c1 指数 e1 模 n1。

在分散子系统中，链接在于当 c2 还没有被前面的步骤 d)完全恢复时开始解码步骤 e)，并且当 c1 还没有被步骤 e)完全恢复时开始解码步骤 f)。优点是能够阻止对例如首先在步骤 e)结束时在分散子系统内析取密报 c1 的攻击，以便将它与明文数据 m 比较，然后用 c1 和 m 攻击算法 A1′，然后逐渐回塑到编码链接。

在安装在保密物理环境中的编码子系统中不需要链接。另一方面它在分散子系统中是有用的。在付费观看的电视的情形中，事实上将 IRD 安装在用户住址上，并且可能是上面描述的那种类型的攻击的目标。最好使 3 个链接的解码算法 A1′，S′和 A2′的组合的攻击比如果密报 c1 和 c2 在每个步骤 d)，e)和 f)之间完全被重建有小得多的成功机会。然而，使用具有公开密钥 e1，n1 和 e2，n2 的算法 A1′和 A2′这个事实意味着在分散子系统中需要的计算方法当与在编码子系统中的计算方法比较时减少了很多。

用例子和固定情况，步骤 a)和 c)，也就是说，具有专用密钥的加密步骤比具有公开密钥的解密步骤 d)和 f)长 20 倍。

在本发明的一个从上面实施例导出的特定实施例中，算法 A1 和 A2 与它们的配对物 A1′和 A2′是相同的。

在本发明的一个也从上面实施例导出的特定实施例中，在步骤 c) 用非对称算法 A2 的公开密钥 e2，n2，而在步骤 d)用这个算法的专用密钥 d2 对密报 c3 进行解密。当依据计算能力远没有得到分散子系统的资源时这个实施例构成一个可能的变体。

虽然芯片卡主要用于解密数据，但是也有一些芯片卡具有进行加密操作所需的能力。在这种情形中，上述的攻击也将与这些离开受到保护的位置如一个管理中心进行工作的加密卡有关。这就是为什么根据本发明的方法也可应用于连续的加密操作，即一当由上游模块传递的信息的一部分可以利用时，下游模块就开始它的加密工作。这个过程的优点是可以交错许多不同的加密模块，因此在给定时间来自上游模块的结果不是

全部可以利用的。然而，下游模块不用完全的结果而是靠部分结果开始它的工作，从而使得对于一个已知的输入状态或输出状态说明一个模块的工作方式是不能实行的。

我们将用下面的通过不受限制的例子取得的附图较详细地了解本发明，其中：

图 1 表示加密操作。

图 2 表示解密操作。

图 3 表示另一种可能的加密方法。

在图 1 中，将数据组 m 引入加密链。第 1 个元素 A1 用由指数 d1 和模 n1 组成的所谓的专用密钥实施加密操作。这个操作的结果由 C1 表示。根据本发明的工作模式，一当结果 C1 的一部分可以利用时，下一个模块就开始工作。这下一个模块 S 用一个秘密密钥实施它的加密操作。一当它部分可以利用时，将结果 C2 传输给模块 A2 以便用由指数 d2 和模 n2 组成的所谓的专用密钥实施第 3 个加密操作。这个最后的结果，这里称为 C3，已准备好通过已知路径如无线电波或电缆被传输出去。

图 2 表示由 3 个解密模块 A1′，S′，A2′组成的解密系统，这 3 个解密模块与用于加密的那些模块相似但是次序相反。这样，我们首先从模块 A2′开始，模块 A2′根据由指数 d2 和模 n2 组成的所谓的公开密钥实施它的解密操作。以对于加密的相同方式，一当来自模块 A2′的结果 C2 的一部分可以利用时，就将它传输给模块 S′以便进行第 2 个解密操作。为了结束解密，模块 A1′根据由指数 e1 和模 n1 组成的所谓的公开密钥实施它的操作。

在本发明的一个特定实施例中，两个模块 A1 和 A2 的密钥是相同的，也就是说在加密时，d1 = d2 和 n1 = n2。类似地，当解密时，e1 = e2 和 n1 = n2。在这种情形中，我们谈到专用密钥 d，n 和公开密钥 e，n。

在本发明的另一个实施例中，如图 3 和 4 所示，模块 A2 用所谓的公开密钥而不用所谓的专用密钥。在加密时，模块 A2 用公开密钥 e2，n2（请参见图 3）进行操作，当解密时（请参见图 4），模块 A2′用专用密钥 d2，n2 进行操作。尽管这种配置显示了对于解密组的总的工作情况，

但是使用专用密钥增强了由模块 A2 提供的保密性。

图 3 和 4 所示的例子不对其它的组合产生限制。例如，可以如此配置模块 A1，使它用公开密钥进行加密操作并用专用密钥进行解密操作。

也可以用具有与模块 A1 和 A2 相同的类型的非对称密钥那类模块代替具有秘密密钥 S 的加密/解密模块。

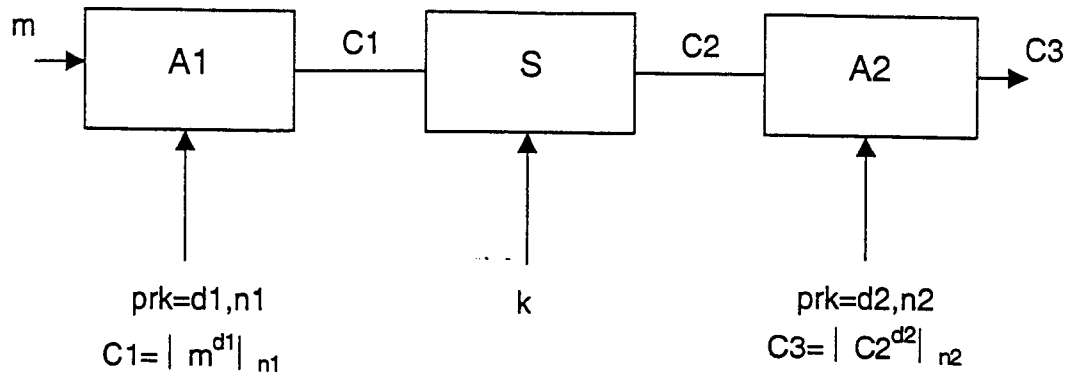

m
A1
C1
S
C2
A2
C3
prk=d1,n1
C1=| m^d1| n1
k
prk=d2,n2
C3=| C2^d2| n2

图 1

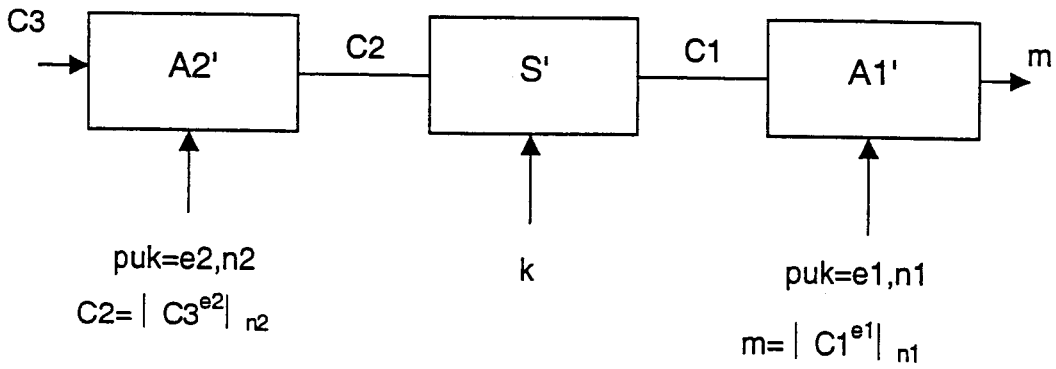

C3
A2'
C2
S'
C1
A1'
m
puk=e2,n2
C2=| C3^e2| n2
k
puk=e1,n1
m=| C1^e1| n1

图 2

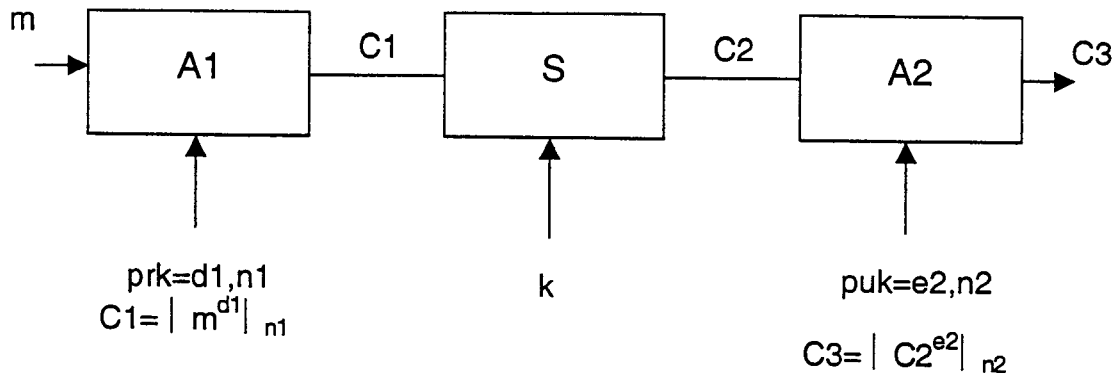

m
A1
C1
S
C2
A2
C3
prk=d1,n1
C1=| m^d1| n1
k
puk=e2,n2
C3=| C2^e2| n2

图 3

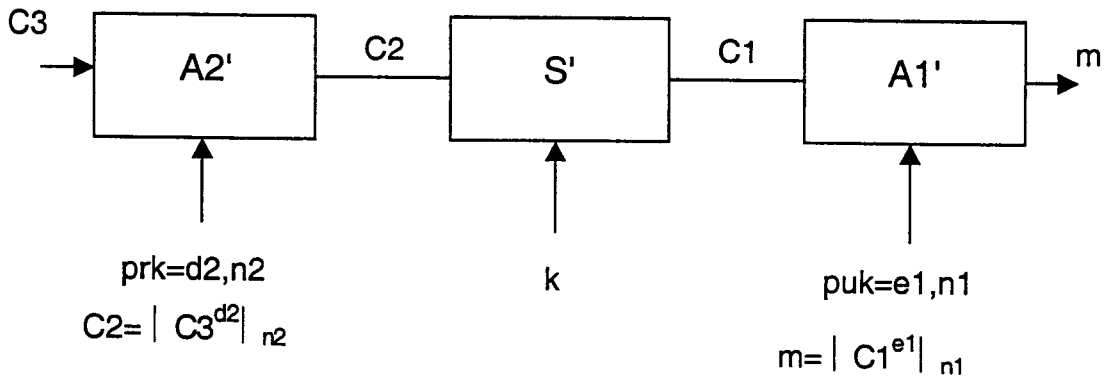

C3
A2'
C2
S'
C1
A1'
m
prk=d2,n2
C2=| C3^d2| n2
k
puk=e1,n1
m=| C1^e1| n1

图 4