

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/30 (2006.01)



[12] 发明专利说明书

专利号 ZL 01807332.8

[45] 授权公告日 2006 年 8 月 16 日

[11] 授权公告号 CN 1270472C

[22] 申请日 2001.3.16 [21] 申请号 01807332.8

[30] 优先权

[32] 2000. 3. 28 [33] FR [31] 00/03919

[86] 国际申请 PCT/FR2001/000796 2001.3.16

[87] 国际公布 WO2001/074006 法 2001.10.4

[85] 进入国家阶段日期 2002.9.27

[71] 专利权人 格姆普拉斯公司

地址 法国热姆诺

[72] 发明人 P·派利尔

审查员 刘冀鹏

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 吴立明 王忠忠

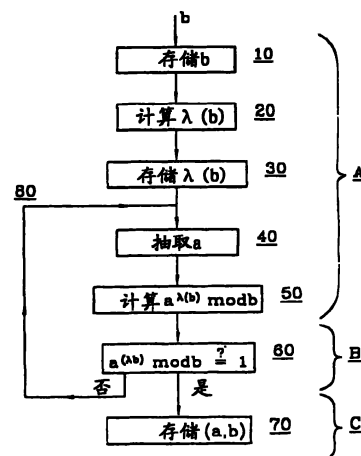
权利要求书 1 页 说明书 4 页 附图 1 页

[54] 发明名称

由互质数产生电子密钥的装置及方法

[57] 摘要

本发明涉及由两个整数 a , b 产生电子密钥的方法, 该方法包括验证所述数 a , b 的互质性的步骤。根据本发明, 该验证步骤包括以下操作: A) - 计算模量乘幂 $a^{\lambda(b)} \bmod b$, 其中 λ 是卡米歇尔函数, B) - 验证该模量乘幂等于 1, C) - 当相等被验证时, 存储该数对 a , b 及在相反情况下用另一数对重复地进行。本发明适合于具有运算处理器的微处理器智能卡。



1. 产生用于公共密钥加密系统的电子密钥的方法，该方法包括：
 - 获取一个整数 b ，
 - 产生一个随机整数 a ，
 - 5 -验证整数 a 、 b 对是否互质，
 - 重复上述产生随机整数 a 的步骤和验证整数对 a 、 b 是否互质的步骤直到获得一对互质的整数 a 、 b ，以及
 - 利用上述的互质整数对产生所述电子密钥，
 - 其特征不在于验证上述整数对是否互质包括以下步骤：
 - 10 A) -计算模量乘幂 $a^{\lambda(b)} \bmod b$ ，其中 λ 是卡米歇尔函数，
 - B) -验证该模量乘幂等于 1。
2. 根据权利要求 1 的产生电子密钥的方法，其特征在于：在数 b 预先被给定的情况下，预先计算 $\lambda(b)$ 及将它存储到存储器中。
3. RSA 或 El Gamal 或 Schnorr 密钥的产生方法，其特征在于：
 - 15 它使用根据上述权利要求中任一项权利要求的方法。

由互质数产生电子密钥的装置及方法

5 本发明涉及由互质的整数产生电子密钥的方法及实施该方法的装置。

本发明尤其适合于用于信息编码后/或两个实体之间的认证和/或信息的电子签名的公共密钥密码协议。

它尤其适合于公共密钥密码协议，例如 RSA (Rivest Shamir 及 Adelman), El Gamal, Schnorr, Fiat Shamir 协议。

10 在这种应用场合中，实际上要求产生大的整数（例如可能大于或等于 512 位）来形成一个或多个协议密钥。对于选择这些数以便使它们保持秘密将附有一个条件，即为它们必需是互质数或它们之间互质。

15 实际上，希望产生这些数以便例如实施密码协议的电子装置将以下列公知方式操作：

- 取一个整数（从一个预定的整数集合中选择，或随机抽取），
- 随机地抽取第二个整数 b，
- 执行数 a 及 b 之间的互质性的操作。该操作允许验证所获得的两个整数互为质数。这是通过该装置的中央单元来实现的。为此，该中央单元计算这两个数之间的最大公约数 (pgcd) 及验证其结果等于 1。事实上可以回忆起：当并且仅当最大约数等于 1 时两个数才互为质数。

对此已具有一些利用微处理器计算两个数的 pgcd 的公知技术。

25 作为例子可以列举：“二进制 GCD”，“扩展 GCD”或 Lehmer 方法。尽管这些方法具有优异的渐近复杂性（这就是说可用于特别大字长的数）。但是它们被证实在具有微处理器的卡类型便携式装置上难以编程（因为复杂）及同时对于常用大字长的数（512 位）具有平庸的性能，现在常用大字长的数趋于变大，即 1024 位或更大。

30 本发明旨在克服这个缺点。更具体地，它的目的是获得由两个整数 a, b 产生电子密钥的方法，该方法包括验证所述数 a, b 的互质性的步骤，其主要特征在于包括以下操作的验证步骤：

A) - 计算模量乘幂 $a^{\lambda(b)} \bmod b$ ，其中 λ 是卡米歇尔 (Carmichael)

函数,

B) -验证该模量乘幂等于 1,

其特征还在于:

5 C) -当相等被验证时, 该运算处理器存储该数对 a, b 及在相反情况下用另一数对重复地进行。

根据另一特征:

-选择一个给定长度的整数 b 及将它存储到存储器中,

-随机抽取一个整数 a ,

-计算 $a^{\lambda(b)} \bmod b$,

10 -验证 $a^{\lambda(b)} = 1 \bmod b$ (或 $a^{\lambda(b)} \bmod b = 1$),

-在相等被验证的情况下存储该数 a ,

-在相反情况下, 用另一数 a 来重复上述步骤。

根据另一特征, 在数 b 预先被给定的情况下, 预计算 $\lambda(b)$ 及将它存储到存储器中。

15 本发明适合于 RSA 或 El Gamal, Schnorr 密钥产生方法。

本发明的另一目的是一种便携式电子装置, 它包括运算处理器及相关的程序处理器, 该装置能执行模量乘幂运算, 其主要特征在于: 它包括一个验证给定长度的整数的互质性的程序, 该验证程序执行以下操作:

20 A) -计算模量乘幂 $a^{\lambda(b)} \bmod b$, 其中 λ 是卡米歇尔函数,

B) -验证该模量乘幂等于 1,

其特征还在于:

C) -当相等被验证时该运算程序存储该数对 a, b 及在相反情况下用另一数对进重复。

25 根据另一特征, 在数 b 预先被给定的情况下, 预计算 $\lambda(b)$ 及将它存储到存储器中。

有利地, 该便携式电子装置由具有微处理器的芯片卡组成。

通过阅读以下以非限定性的例子并参照附图给出的说明, 本发明的其它特征及优点将会一目了然, 附图为:

30 -图 1 表示实施本发明的方法的便携式装置如芯片卡的原理图;

- 图 2 表示实施本发明的方法的一个实施例的流程图。

在以下说明中, 以具有微处理器的芯片卡作为该便携式装置的例

子及为了简化将称其为微处理器卡。

在实施密码协议如 RSA 的情况下，将如所述地，必需确定一个用于产生协议的电子密钥的给定长度的、互为质数的整数对。

为了保证产生的数互为质数，将通过微处理器卡实现互质性的验证步骤，该微处理器使用密码协议的密钥产生方法。

实际上在 RSA 的协议中，两个保持秘密的整数应互为质数及各具有通常为 512 位或 1024 位的固定长度。根据该例，两个整数的一个数 b 是从由微处理器卡产生的一个数集中预先选择及存储的一个整数，而另一数是由微处理器卡在执行协议时以随机方式产生的。

为此，微处理器卡具有一个随机数发生器，它能够提供所需字长的整数。

因此在图 1 中表示出一个能够实施根据本发明方法的微处理器卡的功能图。

卡 C 包括一个主处理单元 1，程序存储器 3 及 4 以及一个与单元 1 相关的工作存储器（未示出）。该卡还包括一个能够执行模量乘幂计算的运算处理器 2。它例如可涉及由 STMicroelectronics 公司出售的电路 ST16CF54 或 Philips 公司的电路 83C852/5。该卡还具有一个随机整数发生器 5。

根据本发明，验证整数互质性的操作由图 2 所示的步骤 A 及 B 来实现，其中具有在这些数互为质数的情况下保留用于产生电子密钥的数对 a, b 的步骤。实际上，该步骤在于将数对 a, b 存储到运算处理器 2 的保安存储器 6 中（不能从外部访问）。

在描述根据本发明的在协议 RSA 的情况下的实施例前，应指出函数 λ 是卡米歇尔函数及该函数由下列关系式确定：

$$\lambda(b) = \text{PPCM}(\lambda(p^{\delta_1}), \dots, \lambda(p^{\delta_k})),$$

其中 PPCM 表示最小公倍数，

其中 $b = \prod p_i^{\delta_i}$ ，该式中每个 p_i 是一个质数及每个 δ_i 是一个非零正整数及 $1 < i < k$ 。

在所示的 RSA 密码协议的例子中，进行以下步骤：

- 存储所选择的固定给定字长的整数 b ， (10)
- 计算 $\lambda(b)$ (20)
- 存储 $\lambda(b)$ (30)

在 b 是预先已知的范围上这些步骤可在以下步骤前进行。在该情况下，预计算的值 $\lambda(b)$ 将被存储在运算处理器的保安存储器 6 中。

- 抽取一个随机整数 a (40)
- 5 -计算 $a^{\lambda(b)} \bmod b$ (50)
- 将 $a^{\lambda(b)} \bmod b$ 与 1 相比较 (60)
- 如果相等，存储该数对 (a, b) ，以便产生密码协议的密钥 (70)
- 如果不相等 (80)
- 10 则从抽取一个新的整数 a 开始来重复上述步骤。

