



[12] 发明专利申请公开说明书

[21] 申请号 01808481.8

[43] 公开日 2003 年 6 月 25 日

[11] 公开号 CN 1426645A

[22] 申请日 2001.4.18 [21] 申请号 01808481.8

[30] 优先权

[32] 2000. 4. 25 [33] FR [31] 00/05254

[86] 国际申请 PCT/FR01/01194 2001.4.18

[87] 国际公布 WO01/82525 法 2001.11.1

[85] 进入国家阶段日期 2002.10.23

[71] 申请人 格姆普拉斯公司

地址 法国热姆诺

[72] 发明人 D·纳卡切 N·达布斯

[74] 专利代理机构 中国专利代理(香港)有限公司

代理人 杨 凯 陈 霁

权利要求书 2 页 说明书 5 页

[54] 发明名称 计算密钥控制数据的方法

[57] 摘要

本发明涉及一种用于计算 N 比特秘密密钥算法的控制数据的方法,其中包括 N—N/n 个随机加密比特以及 N/n 个校验和比特。本发明的特征在于它包括以下步骤:用密钥的 N—N/n 个加密比特对 K 比特的特定信息进行加密;从 K 比特加密消息中选择 N/n 个比特构建控制数据;将所述控制数据的 N/n 比特之一组合到所有 n—1 个加密比特中,以构建完整的 N 比特秘密密钥。本发明特别适用于数据加密标准(DES),所述控制数据是根据常数消息构建的。

I S S N 1 0 0 8 - 4 2 7 4

1. 一种为 N 比特秘密密钥算法计算校验数据的方法，所述秘密密钥中， $N-N/n$ 个比特为随机加密比特，并且 N/n 个比特为校验数据
5 比特，其特征在于，它具有以下步骤：

— 利用所述密钥的所述 $N-N/n$ 个加密比特对 K 比特的特定消息
(M) 进行加密；

— 通过从所述加密消息 (M') 的所述 K 比特中选择 N/n 比特来构建校验数据 (Co)；

10 — 在每 $n-1$ 个加密比特之处结合所述校验数据 (Co) 的所述 N/n 比特之一，以构建完整的 N 比特秘密密钥。

2. 如权利要求 1 所述的计算校验数据的方法，其特征在于：所述特定消息 (M) 为常数消息。

3. 如权利要求 2 所述的计算校验数据的方法，其特征在于：所述
15 常数消息 (M) 的所有输入比特具有相同的值。

4. 如权利要求 1 至 3 之一所述的计算校验数据的方法，其特征在于：所述校验数据 (Co) 由所述加密消息 (M') 的所述前 N/n 个比特组成。

5. 如权利要求 1 至 4 之一所述的计算校验数据的方法，其特征在
20 于： K 等于 N 。

6. 如以上任一权利要求所述的计算校验数据的方法，其特征在于：所述秘密密钥算法为 DES (数据加密标准)，所述密钥具有 64 比特，其中 56 比特为加密比特，并且 8 比特为校验数据比特。

7. 如以上任一权利要求所述的计算校验数据的方法，所述秘密
25 密钥算法以电子元件实现，其特征在于：对每个密钥只进行一次所述校验数据 (Co) 的所述构建。

8. 如权利要求 7 所述的方法，其特征在于：在制造配备了所述密钥的所述电子元件时构建所述校验数据 (Co)。

9. 如权利要求7所述的方法, 其特征在于: 在第一次使用配备了所述密钥的所述电子元件时构建所述校验数据(C_0)。

10. 如以上任一权利要求所述的计算校验数据的方法, 其特征在于: 它还包括通过将根据所述特定消息(M)重新算得的校验数据(C_1)与
5 所述已构建校验数据(C_0)进行比较来验证所述整个秘密密钥的完好性。

11. 如权利要求10所述的方法, 以电子元件实现所述秘密密钥算法, 其特征在于: 在每次电子元件加电时进行所述校验数据($C_1 = C_0$)的验证。

10 12. 如权利要求10所述的方法, 其特征在于: 在每次调用所述算法之前进行所述校验数据($C_1 = C_0$)的验证。

13. 如权利要求10至12之一所述方法, 其特征在于: 它具有在所述校验数据验证出错($C_1 \neq C_0$)时禁止具有所述构建的完整秘密密钥的所述算法的功能。

15 14. 如权利要求10至12之一所述的方法, 以电子元件实现所述秘密密钥算法, 其特征在于: 所述方法具有在所述校验数据验证出错($C_1 \neq C_0$)时禁止使用所述元件的功能。

15. 一种智能卡类型的安全媒体, 其特征在于: 它具有能够实现权利要求1至14所述方法的电子元件。

20 16. 一种配备了加密软件的计算机类型的计算装置, 其特征在于: 它具有能够实现权利要求1至13所述方法的电子元件。

计算密钥控制数据的方法

5 本发明涉及一种为秘密密钥密码算法计算校验数据的方法。这种校验数据主要应用于 DES（数据加密标准）环境中；它在秘密密钥上附加了冗余的特定值，也被称为“校验和”。根据本发明的方法基于从特定（已知并且最好为常数）消息来计算校验数据。在本文以下部分中，将使用惯用词“校验和”来命名该校验数据。

10 更具体地说，本发明涉及 DES 算法，DES 算法实际上是目前已知的唯一利用校验和计算的秘密密钥算法，本发明的目的即是校验和。

 DES 是最著名的、也是使用得最多的秘密密钥密码算法之一。
15 据说这种算法是对称的，因为它使用了秘密且可逆的单 64 比特密钥，用于加密和解密数据。

 更具体地说，DES 具有由 64 个秘密比特组成的密钥，其中包括 56 个随机加密（和解密）比特和 8 个校验和比特。工作时，DES 从这 56 个随机比特中生成 48 比特的 16 个子密钥。这样，在 8 个八比特组的 DES 密钥中的每一个中，前 7 个比特是随机的，用来计算子
20 密钥，而最后一个比特构成了校验和的一部分。一般情况下，该校验和的比特是奇偶校验比特，也就是说，它们是通过对各八比特组中的前 7 个比特进行“异或”运算来计算的。

 校验和主要用于保护 DES 密钥不受存储攻击或 DFA（各种错误
25 攻击），它们会逐一修改密钥的比特，从而试图破解密钥。例如：为 1 的比特被逐个强行归 0，用 DES 进行这些修改，以对同一消息进行加密，直至密钥的全部比特都为 0（此时加密消息为常量）。然后该过程通过回到加密消息链继续，并能成功地判断出在初始密钥

中哪些比特为 1。

校验和使避免这类攻击成为可能。这是因为可以定期重新计算校验和（常规由奇偶校验比特组成），从而可以检测出密钥中一个或多个比特的修改。

- 5 , 另一方面，校验和的知识可以通过揭示出各八比特组中比特为 1 的比特数量是奇数还是偶数来允许对密钥的加密比特上的信息进行过滤。

10 本发明的目的是解决该缺点，并提议了一种计算校验和的方法，这种方法不会泄漏有关密钥的秘密比特的任何信息。

为此，本方法提议从特定消息构建校验和，只使用密钥的加密比特进行编码，并将该校验和的比特结合到密钥的加密比特中，从而重建完整密钥。然后根据传统运算使用算法，其中密钥包括随机加密比特和这个构建的校验和。

15 本发明更具体的目的是一种为 N 比特秘密密钥算法计算校验数据的方法，其中 $N-N/n$ 为随机加密比特， N/n 为校验数据比特，其特征在于，它具有以下步骤：

- 利用密钥的 $N-N/n$ 加密比特对 K 比特的特定消息进行加密；
- 通过从所述 K 比特加密消息中选择 N/n 比特来构建校验数据；
- 20 - 在密钥的每 $n-1$ 个加密比特之处结合所述校验数据的 N/n 比特之一，以构建完整的 N 比特秘密密钥。

根据一个特征，所述特定消息为常数消息。

根据一个特定特性，所述常数消息的 K 个输入比特具有相同值。

根据另一特征，所述校验数据包括加密消息的前 N/n 个比特。

25 根据一个特征， K 等于 N 。

根据一个优选应用，秘密密钥算法为 DES，所述密钥具有 64 比特，其中 56 个为加密比特，8 个为校验数据比特。

根据一个特征，秘密密钥算法用电子元件实现，每个密钥的校

验数据的构建只进行一次，时间为制造电子元件时，或在第一次使用具有给定密钥的该电子元件时。

根据一个特征，本方法还包括通过将根据同一特定消息重新算得的校验数据与构建的校验数据进行比较来验证整个秘密密钥的完好性。

根据一个特征，每次电子元件加电时对校验数据进行验证。

根据另一特征，每次调用算法之前对校验数据进行验证。

根据一个特征，当校验数据的验证出错时，本方法具有禁止具有构建的秘密密钥的算法的功能和/或禁止电子元件的功能。

10 本发明适用于各种智能卡类型的安全媒体，或各种配有加密软件的计算机类型的计算装置，它们具有能够实现根据本发明的方法的电子元件。

根据本发明的方法使构建校验和成为可能，它不会揭示任何与秘密密钥相关的信息。这是因为校验和不再以任何方式与密钥的加密比特的奇偶校验相关联。

15 此外，因为本校验和不含任何敏感信息，因此甚至没有将其隐藏的必要。

密钥的安全型仍然是肯定的，因为通过计算新校验和并将其与最初构建的校验和进行比较，保留了未出现攻击的验证。

20 根据本发明的方法要求算法的第一次运算只使用密钥的加密比特，以便重新计算校验和来进行验证，这样做是耗时的。不过，根据本发明的方法用安全上的收获补偿了这个时间成本。

25 通过阅读下面说明性的而非限制性的例示的描述，本发明的其它特定特性及优点会清楚地显露出来。

本说明书涉及具有 64 比特的秘密密钥的 DES 算法。这是因为在目前已知的算法当中，只有 DES 使用校验和来计算 DFA 类型的存储攻击。不过，根据本发明的方法也可以应用到其它使用可能更长

的秘密密钥的对称算法上。

本发明的目的是构建一种不会暴露 DES 密钥的 56 个加密比特的任何信息的校验和。

5 为此，由 DES 的 56 个加密比特对 K 比特的特定消息 M、即未加密的消息 M 进行编码。根据一个优选实现例，选择含有 64 个常数的、即固定且已知比特的消息 M。根据一个实现例，消息 M 可包括全部具有相同值的 K 个比特，例如都是 0。DES 输出的加密消息 M' 具有 K 个比特（本例示中为 64 个），它绝对没有泄漏算法中用到的 56 个加密比特的任何信息。

10 因此，本发明包括从加密消息 M' 的 64 个比特中选择 8 个比特。尽管选择任何比特都可以，但是为了简单，最好选择前 8 个，即加密文本 M' 的第一个八比特组。这 8 个比特接下来就组成了 DES 校验和 Co。

15 组成的这个校验和 Co 的比特接下来被组合到 56 个随机加密比特中，以形成一个完整的 64 比特密钥。每隔 7 个比特的加密比特之间放置校验和的一个比特。

20 对某一给定密钥只这样构建校验和 Co 一次，而且为所有给定密钥都进行校验和的构建，或者是在实现 DES 的电子元件的生产制造结束时，或者是在首次与该密钥一起使用所述元件时。实际上，存在 DES 密码可以被修改的应用，这时就需要重建校验和 Co。

结果是，DES 重新开始传统运算，也就是说，它用 64 比特密钥来对消息进行编码和解码，密钥中 56 比特为随机的，另外 8 比特为校验和，其中绝对没有包括有关所述加密比特的任何信息。

25 不过，例如每次对元件加电时，或者每次调用 DES 之前，通过重新计算校验和 C_1 并将其与已构建的校验和 Co 进行比较，对可能的 DFA 类型的存储攻击的保护仍然是肯定的。

验证校验和 C_1 是利用来自初始常数消息 M 的 56 个加密比特的密钥进行计算的，并由加密消息 M' 的 8 个比特确定（与 Co 的比特

相同，比如再次使用第一组）。

若发生了 DFA 攻击，且密钥的某个比特被修改了，则利用来自同一初始常数消息 M 的被攻击密钥算得的校验和 C_1 将必然与初始构建并储存的 C_0 不同。这是因为，由于 DES 是一种非线性算法，所以修改密钥的一个比特将会改变加密消息 M' 的许多比特，并且从该被攻击密钥重建的校验和 C_1 肯定会有比特与 C_0 不同。

另一方面，若 $C_1 = C_0$ ，则密钥没有受到任何攻击，可放心使用。

相反，若 $C_1 \neq C_0$ ，则密钥受到了攻击。根据本发明的方法具有禁止使用具有这个构建的完整密钥的加密/解密算法的功能和/或禁止使用安装了本方法的电子元件的功能（如智能卡）。