



(12) 发明专利

(10) 授权公告号 CN 1748385 B

(45) 授权公告日 2012. 08. 29

(21) 申请号 200380109671. 1

(22) 申请日 2003. 12. 10

(30) 优先权数据

10258323. 4 2002. 12. 13 DE

(85) PCT申请进入国家阶段日

2005. 08. 11

(86) PCT申请的申请数据

PCT/EP2003/014015 2003. 12. 10

(87) PCT申请的公布数据

W02004/056035 DE 2004. 07. 01

(73) 专利权人 德国捷德有限公司

地址 德国慕尼黑

(72) 发明人 赫尔曼·德雷克斯勒

拉尔斯·霍夫曼 于尔根·普尔库斯

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 邵亚丽 李晓舒

(51) Int. Cl.

H04L 9/06 (2006. 01)

(56) 对比文件

全文.

FR 2810438 A1, 2001. 12. 21, 全文.

WO 99/14889 A1, 1999. 03. 25, 全文.

CA 2327037 A1, 2002. 05. 22, 全文.

CN 1245925 A, 2000. 03. 01, 说明书第 2 页第 25 行至第 3 页第 6 行、权利要求 1.

丁一强. 基于 CCS 的加密协议分析. 软件学报 10 10. 1999, 10(10), 1103-1107.

审查员 李晓莉

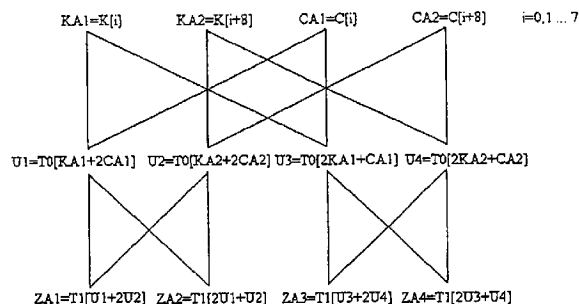
权利要求书 6 页 说明书 12 页 附图 3 页

(54) 发明名称

加密方法

(57) 摘要

本发明涉及一种用于提高在加密方法中防止确定密钥的安全性的方法, 其中, 加密方法通过对输入数据、即明文和密钥应用加密算法计算出密文, 其中对输入数据预先或在本方法期间进行检查和分析, 对该密钥和明文应用加密算法, 以根据该分析计算出密文或在密文计算路径中的中间结果。



1. 一种用于提高在加密方法中防止确定密钥的安全性的方法,在该加密方法中通过对包含明文和密钥的输入数据应用加密算法来计算出密文,其中在所述方法中,
根据预定的判断准则对该明文进行检查,和 / 或预先进行检查,
根据该检查对该明文进行分析,并且
对该密钥和明文应用加密算法,以根据该分析计算出密文或在该密文的计算路径上的中间结果,其中所述分析包括,从明文中获得关于攻击能确定密钥的加密算法的信息。
2. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,所述分析包括从明文中获得关于将来对加密算法的攻击的信息。
3. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,由该分析宣布出现了冲突,其中冲突的出现在于,两个不同的明文在用相同的密钥和相同的加密算法进行加密时提供一致的密文,或在从明文到密文的计算路径中的任意特定位置上提供一致的中间结果。
4. 根据权利要求 3 所述的用于提高安全性的方法,其特征在于,根据所述分析对加密算法的应用包括,考虑具有冲突的密钥和 / 或属于这种密钥的冲突明文对。
5. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,所述分析包括,分析明文是否包含关于在该用于提高安全性的方法运行期间已经对加密算法进行的攻击的信息。
6. 根据权利要求 5 所述的用于提高安全性的方法,其特征在于,按照权利要求 5 的所述信息具有明文的一致性,该一致性是指,所述明文至少部分地与先前在执行加密算法时被引入该加密算法的明文一致。
7. 根据权利要求 6 所述的用于提高安全性的方法,其特征在于,对于所述检查采用测试输入数据,并且在该用于提高安全性的方法中采用的输入数据在执行该用于提高安全性的方法之后作为用于检查的新测试输入数据而提供给随后进行的该用于提高安全性的方法的其它实施。
8. 根据权利要求 7 所述的用于提高安全性的方法,其特征在于,将已经通过检查和 / 或用于检查的待剔除的测试输入数据替换为新输入数据,其中待剔除的测试输入数据在随后进行的检查中不再作为测试输入数据用于实施检查。
9. 根据权利要求 3 或 4 所述的用于提高安全性的方法,其特征在于,所述明文具有至少一个子明文,密钥具有至少一个子密钥,其中在该用于提高安全性的方法中,
 - 在计算步骤中对明文的至少一个子明文和密钥的至少一个子密钥应用加密算法的至少一部分,从而计算出加密结果,该结果被提供为密文或至少被提供为可以通过其它计算步骤计算出该密文的中间结果,以及
 - 这样选择该密钥,使得其用于每一个子明文的每一个子密钥都具有相应预定次数的冲突,其中从可能冲突次数的预定集合中确定用于每个子密钥的次数。
10. 根据权利要求 9 所述的用于提高安全性的方法,其特征在于,每个子密钥分别具有预定的最高次数的冲突。
11. 根据权利要求 10 所述的用于提高安全性的方法,其特征在于,相应的预定冲突最高次数对每个子密钥都是相同的。
12. 根据权利要求 10 所述的用于提高安全性的方法,其特征在于,所述子密钥没有冲突。

13. 根据权利要求 10 所述的用于提高安全性的方法,其特征在于,所述预定的最高次数的冲突为一次冲突。

14. 根据权利要求 9 所述的用于提高安全性的方法,其特征在于,所述子密钥是密钥本身。

15. 根据权利要求 9 所述的用于提高安全性的方法,其特征在于,所述子明文是明文本身。

16. 根据权利要求 9 所述的用于提高安全性的方法,其特征在于,至少一个子密钥具有至少一次冲突。

17. 根据权利要求 16 所述的用于提高安全性的方法,其特征在于,在采用加密算法之前检查子明文是否属于一个冲突的子明文对,针对该子明文对至少一个子密钥具有至少一次冲突,以及其中,如果检查给出该子明文属于一个这样的冲突的子明文对,则基于该检查而对于来自该冲突子明文对的至少两个子明文之一,防止将采用具有子密钥和来自该冲突对的子明文的加密算法而获得的加密结果提供为密文或中间结果。

18. 根据权利要求 17 所述的用于提高安全性的方法,其特征在于,基于所述检查而对于来自所述冲突子明文对的至少两个子明文之一,不对该子明文应用具有该子密钥的加密算法。

19. 根据权利要求 17 或 18 所述的用于提高安全性的方法,其特征在于,对来自冲突对的至少一个子明文,不提供加密结果,而提供证明文本作为密文或中间结果。

20. 根据权利要求 19 所述的用于提高安全性的方法,其特征在于,防止提供加密结果仅对来自所述冲突子明文对的两个子明文之一实施,其中对于来自该冲突子明文对的两个子明文中的另一个,将通过采用包括子密钥和子明文的加密算法计算出的加密结果提供为密文或中间结果。

21. 根据权利要求 19 所述的用于提高安全性的方法,其特征在于,利用对相应的子明文检查其是否属于一个冲突的子明文对,对整个明文检查其是否属于一个冲突的明文对,其中所述子明文构成该明文的至少一部分。

22. 根据权利要求 19 所述的用于提高安全性的方法,其特征在于,在所述检查之前从存储器中读取所述冲突子明文对的至少一部分和 / 或分别读取每一个这样的对中的至少一部分。

23. 根据权利要求 19 所述的用于提高安全性的方法,其特征在于,在所述检查之前从存储器中读取该冲突明文对的至少一部分和 / 或分别读取每一对的至少一部分。

24. 根据权利要求 23 所述的用于提高安全性的方法,其特征在于,所述冲突子明文对与明文一起从存储器中读取,其中这些子明文分别构成该明文的至少一部分。

25. 根据权利要求 24 所述的用于提高安全性的方法,其特征在于,所述证明文本通过用一个与密钥或子密钥不同的证明密钥或证明子密钥对明文或子明文采用加密算法而计算出来。

26. 根据权利要求 24 所述的用于提高安全性的方法,其特征在于,所述证明文本通过对明文或子明文采用与加密算法不同的证明算法计算出来。

27. 根据权利要求 24 所述的用于提高安全性的方法,其特征在于,所述证明文本是随机提供的文本。

28. 根据权利要求 24 所述的用于提高安全性的方法,其特征在于,在经过一个预定的证明时间间隔之后才提供所述证明文本。

29. 根据权利要求 28 所述的用于提高安全性的方法,其特征在于,所述证明时间间隔这样设置,使得证明文本的提供基本上与应用和至少部分运行加密算法持续得一样长,加密算法的结果根据检查由提供证明文本来代替。

30. 根据权利要求 9 所述的用于提高安全性的方法,其特征在于,在所述中间结果中出现相应的预定次数的冲突。

31. 根据权利要求 30 所述的用于提高安全性的方法,其特征在于,所述加密算法具有至少两次子循环,其中从至少两次子循环中计算出所述中间结果作为一次预定子循环的结果,从而在预定子循环之后出现预定次数的冲突。

32. 根据权利要求 31 所述的用于提高安全性的方法,其特征在于,在所述第二次子循环之后出现预定次数的冲突。

33. 根据权利要求 9 所述的用于提高安全性的方法,其特征在于,所述密钥分为多个子密钥,明文分为多个子明文,其中从一个子密钥和一个子明文计算出一个子中间结果,以及其中对于一个预定的子密钥和至少一对子明文出现预定数量的冲突。

34. 根据权利要求 5 所述的用于提高安全性的方法,其特征在于,在该方法中,
- 实施至少一个检查步骤,其中根据预定的一致性判断准则检查所述明文是否与测试明文一致,以及
- 如果在该至少一个检查步骤中确定对应的一致性,则计数器增一,以及
- 只要计数器的值小于预定的最大计数值,就在计算步骤中对明文或至少明文的一部分以及密钥或至少密钥的一部分应用加密算法的至少一部分,从而计算出加密结果,该结果被提供为密文或至少提供为可以通过其它计算步骤计算出密文的中间结果。

35. 根据权利要求 34 所述的用于提高安全性的方法,其特征在于,所述明文具有至少一个子明文,测试明文具有至少一个子测试明文,其中根据预定的一致性判断准则,如果明文和测试明文的不同之处最多在于该至少一个子明文与该至少一个子测试明文相互不同并且除此之外相互一致,则在这种情况下确定为一致。

36. 根据权利要求 34 或 35 所述的用于提高安全性的方法,其特征在于,所述明文具有内部数量的子明文,测试明文具有内部数量的子测试明文,其中根据预定的一致性准则,如果明文和测试明文的不同之处最多在于一个子明文与一个子测试明文相互不同并且除此之外相互一致,则在这种情况下确定为一致。

37. 根据权利要求 36 所述的用于提高安全性的方法,其特征在于,每个子明文和每个子测试明文都是两字节长,其中根据预定的一致性判断准则,如果明文和测试明文最多有两个字节相互不同,则在这种情况下确定为一致。

38. 根据权利要求 36 所述的用于提高安全性的方法,其特征在于,用多个测试明文进行多个检查步骤。

39. 根据权利要求 38 所述的用于提高安全性的方法,其特征在于,所述计数器在根据预定的判断准则对所述多个检查步骤的至少部分检查步骤确定一致时才增一。

40. 根据权利要求 39 所述的用于提高安全性的方法,其特征在于,所述计数器在根据预定的判断准则确定至少一个所述检查步骤一致时才增一。

41. 根据权利要求 39 或 40 所述的用于提高安全性的方法,其特征在于,在所述检查步骤之前用测试明文执行至少一个在前的计算步骤,其中在该在前的计算步骤中对该测试明文或至少一个子测试明文以及密钥或至少一个子密钥应用加密算法的至少一部分,从而计算出测试加密结果,其中该测试明文在该在前的计算步骤之后作为测试明文提供给检查步骤。

42. 根据权利要求 39 或 40 所述的用于提高安全性的方法,其特征在于,在用明文或至少一个子明文执行了计算步骤之后将该明文作为后续测试明文提供给后面进行的其它检查步骤。

43. 根据权利要求 42 所述的用于提高安全性的方法,其特征在于,由后续测试明文来替换已经用于检查步骤和 / 或已在该检查步骤中使用的待剔除的测试明文,其中该待剔除的测试明文在随后的一个检查步骤中不作为用于执行检查步骤的测试明文。

44. 根据权利要求 41 所述的用于提高安全性的方法,其特征在于,用多个测试明文执行多个在前的计算步骤,其中对测试明文或至少一个子测试明文以及密钥或至少一个子密钥分别应用加密算法的至少一部分,从而计算出多个测试加密结果,其中每个测试明文在相应的在前的计算步骤之后用于至少一个检查步骤。

45. 根据权利要求 44 所述的用于提高安全性的方法,其特征在于,将来自多个测试明文的、在多个检查步骤中作为测试明文采用次数最多的测试明文作为待剔除的测试明文替换掉。

46. 根据权利要求 43 或 44 所述的用于提高安全性的方法,其特征在于,将来自多个测试明文的、最早用作后续测试明文的测试明文作为待剔除的测试明文替换掉。

47. 根据权利要求 46 所述的用于提高安全性的方法,其特征在于,所述后续测试明文是从明文转换为测试明文。

48. 根据权利要求 34 所述的用于提高安全性的方法,其特征在于,所述最大计数值是 1。

49. 根据权利要求 48 所述的用于提高安全性的方法,其特征在于,采用比较单元作为计数器,用于在确定一致的情况下防止将加密结果提供为密文或中间结果。

50. 根据权利要求 34 所述的用于提高安全性的方法,其特征在于,所述最大计数值是 12。

51. 根据权利要求 34 所述的用于提高安全性的方法,其特征在于,当计数器值达到或超过预定的最大计数值时,不提供加密结果而提供证明文本作为密文或中间结果。

52. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,所述密钥是二进制或十六进制编码的密钥。

53. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,将所述密钥分为多个子密钥,将所述明文分为多个子明文。

54. 根据权利要求 9 所述的用于提高安全性的方法,其特征在于,每个子密钥都可以由两个底层子密钥、即密钥字节组成,每个子明文都可以由两个底层子明文、即明文字节组成。

55. 根据权利要求 54 所述的用于提高安全性的方法,其特征在于,每个底层子密钥和每个底层子明文分别有一个字节长。

56. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,所述加密算法是对称加密算法。

57. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,所述加密算法是具有密钥的哈希函数。

58. 根据权利要求 1 所述的用于提高安全性的方法,其特征在于,所述加密算法具有 8 次循环。

59. 根据权利要求 58 所述的用于提高安全性的方法,其特征在于,每次循环具有 5 次子循环。

60. 根据权利要求 59 所述的用于提高安全性的方法,其特征在于,所述加密算法是 COMP128-1 算法。

61. 一种将权利要求 1 至 60 中任一项所述用于提高安全性的方法用于防止试图通过重复执行加密算法确定密钥或子密钥的攻击的应用。

62. 根据权利要求 61 所述的应用,其特征在于,对重复执行该算法的次数计数,并在达到执行该加密算法的预定最高次数之后将后续的执行闭锁到至少预定的等待时间间隔过去之后。

63. 根据权利要求 62 所述的应用,其特征在于,所述闭锁仅当执行的预定最高次数出现在预定的时间间隔内时才执行。

64. 根据权利要求 62 或 63 所述的应用,其特征在于,执行的预定最高次数在 20000 到 200000 的范围内。

65. 根据权利要求 64 所述的应用,其特征在于,执行的预定最高次数为 65535 次。

66. 一种用于提高在加密方法中防止确定密钥的安全性的装置,在该加密方法中通过对包含明文和密钥的输入数据应用加密算法来计算出密文,其中在所述装置中,具有

用于根据预定的判断准则对该明文进行检查,和 / 或预先进行检查的装置,

用于根据该检查对该明文进行分析的装置,和

对该密钥和明文应用加密算法,以根据该分析计算出密文或在该密文的计算路径上的中间结果的装置,其中所述分析包括,从明文中获得关于攻击能确定密钥的加密算法的信息。

67. 根据权利要求 66 所述的装置,其特征在于,所述装置具有存储密钥的密钥存储装置。

68. 根据权利要求 67 所述的装置,其特征在于,在所述密钥存储装置中还存储有证明密钥。

69. 根据权利要求 66 所述的装置,其特征在于,所述装置具有明文存储装置,其中针对所述密钥,对于至少一对冲突的明文或子明文存储该两个明文或子明文中的至少一个。

70. 根据权利要求 69 所述的装置,其特征在于,对于每对冲突的明文或子明文都存储来自该对冲突明文或子明文的两个明文或子明文之一。

71. 根据权利要求 66 至 70 中任一项所述的装置,其特征在于,所述装置还具有测试明文存储装置,其中存储至少一个测试明文或至少一个测试子明文。

72. 根据权利要求 66 所述的装置,其特征在于,所述装置还具有用于实施根据权利要求 61 至 65 中任一项所述应用的装置。

73. 根据权利要求 66 所述的装置,其特征在于,在该装置中还至少部分地实现移动电话卡的功能。

74. 一种用于对根据权利要求 66 所述的装置进行个性化的方法,其中在该方法中将密钥存储在装置中,其中这样选择密钥,使得该密钥的每个子密钥对于每个子明文都具有相应预定数量的冲突,其中对于每个子密钥的次数由预定的可能数量的冲突集合确定。

75. 根据权利要求 74 所述的用于对权利要求 66 所述的装置进行个性化的方法,其特征在于,每个子密钥分别具有预定最高次数的冲突。

76. 根据权利要求 75 所述的用于对权利要求 66 所述的装置进行个性化的方法,其特征在于,所述子密钥没有冲突。

77. 根据权利要求 75 所述的用于对权利要求 66 所述的装置进行个性化方法,其特征在于,至少一个子密钥具有至少一次冲突。

78. 根据权利要求 74 至 77 中任一项所述的用于对权利要求 66 所述的装置进行个性化的方法,其特征在于,在该方法中除了所述密钥之外还在该装置中存储冲突明文或子明文中的至少一个。

79. 根据权利要求 74 至 77 中任一项所述的用于对权利要求 66 所述的装置进行个性化的方法,其特征在于,在该方法中还在该装置中这样存储一个证明密钥,使得在基于检查而没有采用所述密钥时,加密算法采用该证明密钥。

加密方法

技术领域

[0001] 本发明涉及一种用于对明文加密的方法和实施该方法的数据载体。

背景技术

[0002] 在加密算法中,采用密钥将明文加密成密文。在此,加密算法的概念应理解为用于计算关于明文的识别码、即所谓的 MAC(消息识别码)的算法。这种算法也称为具有密钥的哈希函数(加密的哈希函数)。在此,采用密钥从明文中计算 MAC。通常,与狭义下的真正加密算法相反,这种函数是不能反向的,也就是说不能再进行解密。

[0003] 加密算法例如用于相对于第二实例验证第一实例。为此,例如第一实例用一个共用的、两个实例都具有的密钥将其先前以未加密的形式从第二实例获得的明文加密成要发送回第二实例的第一密文。第二实例同样用该共用密钥,独立于第一实例的加密地对该明文进行加密,并由此计算出第二密文。如果第一实例实际上将该共用密钥用于加密,则第一和第二密文是一致的。这样,第一实例相对于第二实例自我验证,其中第一实例相对于所获得的明文发回正确的密文。对于该方法的可应用性和可靠性,要求一定要使共用密钥对第三方严格保密。

[0004] 密钥这样来获得,例如在快速计算机上试探由所有密钥构成的密钥空间中的所有可能的密钥。一个 m 位长的二进制密钥的密钥空间的大小是 2^m 。因此,根据密钥长度 m ,为了通过简单的试探来确定密钥需要实施非常多次的加密算法。因此密钥长度 m 一般选择为(例如 $m > 70$)使得这种攻击是不切实际的,因为需要耗费很多年的时间。

[0005] 有效攻击利用了所采用的各种加密算法的某些漏洞。

[0006] 在这种攻击中,加密时采用密钥,并且改变了用该密钥加密的明文。更为准确的是,在这些攻击中聚集多个明文/密文对,也就是由一个明文和一个对应于该明文的密文组成的对子,该密文是通过用加密算法和密码对明文进行加密形成的,这些明文/密文对具有这样的特性,从该明文/密文对中可以获得关于该密码的信息(参见下面)。在特别有效的攻击中,攻击者可以有针对性地选择他想要加密的明文(选择的纯文本攻击),由此明文/密文对的集合可以有针对性地建立并因此更为有效。为了使攻击成功,需要收集关于密钥的足够信息。为此需要对足够多的明文进行加密。因此,必须执行非常多次的加密算法。

[0007] 在特别有效的、利用所采用的加密算法的漏洞的攻击中,利用所谓冲突的出现作为特性,通过该特性可以获得有关密码的信息。冲突一般理解为两个不同的明文在用相同的密钥和加密算法加密时得出相同的加密结果(参见下面)。如果出现这样的冲突,则可以从最终确定出密码。

[0008] 更为确切的是,密钥(恰好)具有一次冲突的特性在本发明中理解为针对该密钥(恰好)只有一对冲突的明文 P_0 、 P_1 ,其加密(其中,两个冲突明文 P_0 、 P_1 中的每一个都被分别加密)通过采用加密算法和该密钥给出相同的密文,或者其部分加密通过部分采用加密算法和密钥或该密钥的一部分,在加密算法的运行序列中的任一预定位置在从明文到密

文的计算路径中给出相同的中间结果。对于一个具有 n 个冲突的密钥,相应的就有 n 对冲突的明文 $(P_{00}, P_{10}), (P_{01}, P_{11}), \dots (P_{0n-1}, P_{1n-1})$, 其中两个冲突的明文 P_{0i}, P_{1i} 在相应的第 i 对在用密钥 (或用该密钥的一部分) 加密时给出相同的密文或相同的中间结果。这种冲突情况是特别令人感兴趣的,即其中存在子明文,其利用一个子密钥产生一个或多个冲突。在这种情况下可以从该 (一个或多个) 冲突中获得关于子密钥的信息。在此,通常通过该子明文形成整个待加密明文的一部分,并且通过该子密钥一般形成整个密钥的一部分。由于子密钥的可能值和子明文的可能值的空间都比整个密钥空间或整个明文空间小,因此可以非常有效地攻击子密钥。然后,可以将对密钥的攻击分为对子密钥的多次攻击,这可以非常有效地实施。用这些子密钥可以重建密钥。这个措施通常比攻击整个密钥来得更为有效。

[0009] 其它可以用来获得关于密码的信息的特殊方法例如是密码分析学方法,如微分和线性密码分析。

[0010] 在用于提高防止在加密方法中确定密钥的安全性的方法中,允许实施的加密的次数限制为预定的最高数。为此借助计数器对执行加密算法的频度进行计数。只要将加密算法实施了预定的最高次数,就将其锁定,不能再重新执行该加密算法。由此试图通过明文/密文对的集合和分析确定密钥的分析者只能尝试有限的次数,该次数可能不足以确定整个密钥。但是通过将加密限制为最高次数也同时限制了加密算法的有效持续时间,因为计数器在每次正规执行加密算法时也只计数到最高数。

[0011] 在另一种提高防止在加密方法中确定密钥的安全性的方法中,将允许执行的加密次数在预定的时间间隔内限制为预定的最高次数。在试图通过收集和分析明文/密文对来确定密钥、也就是通过用始终相同的密钥和多个明文执行加密算法来确定密钥时,在适当选择该时间间隔和最高次数的情况下,如果在该时间间隔内超过最高次数则锁闭加密算法。在经过一段等待时间后重新打开该加密算法。这样就不会限制加密算法的有效持续时间。但在这种方法中,在该时间间隔内还是只能正规实施最高次数的加密算法。这可能导致对用户友好性的限制,因为即使在正规执行加密算法时也必须保持该等待时间。

[0012] 在特别严格的提高防止在加密方法中确定密钥的安全性的方法中,将允许执行加密算法的最高次数在预定时间间隔内设置为一个特别低的值,或者在预先给定允许实施该算法的最高次数的情况下将事件间隔的长度设置为一个特别低的值。或者,执行加密算法的最高次数和时间间隔都分别设置为一个特别低的值。但由此也将可进行的正规实施的次数限制在该时间间隔内。由此极大地限制了加密方法的用户友好性。

[0013] 由文献 CA2327037 公开了一种用于识别对密码算法进行攻击的方法。在该方法中采用多个由一个原始密钥计算出的子密钥。在初始化步骤中,通过子密钥和一个预先固定给出的输入向量计算校验和并作为参考校验和存储。在用该密钥对消息加密的密码算法期间,通过子密钥和输入向量再次计算校验和,并与参考校验和进行比较。如果这两个校验和相互不同,则说明对密码算法的由密钥计算出子密钥的那一部分进行了攻击。参考校验和例如可以在向用户交付智能卡之前就写在该智能卡上。

[0014] 发明内容

[0015] 本发明要解决的技术问题在于,在加密方法中提供一种特别可靠和用户友好的方法来提高防止确定密钥的安全性。

[0016] 该技术问题是通过根据独立方法权利要求或应用权利要求的方法以及根据独立装置权利要求的数据载体解决的。

[0017] 在根据本发明的提高防止确定密钥的安全性的方法中,由加密方法出发,其中通过对明文和密钥采用加密算法而计算出密文。

[0018] 为了提高安全性,将作为用于计算密文的数据而引入该加密算法中的数据在该方法之前或在该方法期间根据预先确定的判断准则进行检查和分析。根据该分析,将用于通过加密算法进行处理的输入数据用于计算密文或在密文计算路径上的中间结果。

[0019] 由此通过本发明的方法,提高了安全性而没有限制容许执行加密算法的次数。因此特别是提高了该方法的用户友好性。

[0020] 作为用于计算密文的输入而引入加密算法的输入数据,可以是密钥或明文,或密钥和明文。可选地,在输入数据中,除了明文之外还对密钥进行检查和分析。

[0021] 尤其是例如根据预定的判断准则选择密钥。此外或作为另一种选择,例如对为了加密而引入加密算法的明文进行根据预定判断准则的检查和析,仅在相应的对该明文分析之后,才允许通过加密算法进行正规的处理,以用于计算密文或在密文计算路径上的中间结果。

[0022] 优选地,明文至少具有一个子明文,密钥至少具有一个子密钥。通常,明文具有多个子明文,密钥具有多个子密钥。

[0023] 优选地,分析包括,从输入数据中获得关于攻击能确定密钥的加密算法的信息。通过将这种信息用于实施本方法,可以有目的地针对能确定密钥的攻击并防止攻击。通过根据该分析来执行加密算法可以实现这种防止。

[0024] 根据本发明方法的第一变形,所述分析包括从输入数据中获得关于将来对加密算法的攻击的信息。优选地,由该分析宣布出现了冲突,其中冲突的出现在于,两个不同的明文在用相同的密钥和相同的加密算法对其进行加密时得出一致的密文,或在从明文至密文的计算路径上的一任意特定位置上给出一致的中间结果。两个这样的明文称为一个冲突的明文对。由一对这样的冲突明文可以限制密钥空间。通过其它类似步骤最后可以确定密钥。在该方法的第一变形中,根据分析对加密算法的应用包括考虑具有冲突的密钥和/或属于这种密钥的冲突明文对。

[0025] 根据本发明方法的第二变形,所述分析包括,输入数据包含关于在本方法运行期间已经对加密算法进行的攻击的信息。

[0026] 在第二变形中,所述信息尤其是具有明文的一致性,该一致性是指,该明文至少部分地与先前在执行加密算法时被引入该加密算法的明文一致。

[0027] 通常,在连续执行加密算法时为了进行验证而出现的明文是随机可变地不同或基本上不协调一致的明文。明文的一致性至少以很大的概率表明,有受到有针对性的操纵的明文输入以实施对加密算法的攻击。

[0028] 对于为了获得分析而进行的检查,优选采用测试输入数据,将输入数据与该测试输入数据进行比较。在用于执行加密算法的方法中采用的输入数据优选在实施该方法之后作为用于检查的新测试输入数据而提供给随后进行的该方法的其它实施。在此,优选在为新输入数据而进行交换时,已经提供给检查和/或用于检查的剔除的测试输入数据被替换,其中待剔除的测试输入数据在随后进行的检查中不再作为测试输入数据用于实施检

查。也就是说,优选在每次执行加密算法时对用于检查的测试输入数据组进行实时更新。

[0029] 可以这样采用根据本发明的方法:对诸如密钥和/或明文的输入数据进行事先有针对性的选择,并利用该有针对性选择的输入数据实施加密算法。这种有针对性的选择可以在每次实施该方法时进行。这种有针对性的选择还可以仅实施一次。对于一种实现在数据载体中的方法和有针对性选择的密钥,可以通过事先用该密钥一次性定制该数据载体来进行有针对性的选择。

[0030] 或者,这样来采用该方法,在每次实施时都检查和分析输入数据。例如,检查和分析输入的明文,并根据该分析应用或不应用或根据更改了的方法应用该明文。更改了的方法例如可以是采用另一种密钥的方法。

[0031] 为了进一步提高该方法的安全性,可以另外限制允许实施该加密算法的次数。在此,由于本发明的安全措施,通常允许执行加密算法的最高次数比没有采用本发明的安全措施时设置得更高,在达到或超过该最高次数时就锁定该加密算法。由此本发明的方法在用限制允许执行加密算法的最高次数构造的实施方式中具有特别高程度的用户友好性。

[0032] 在用于根据本方法的第一变形的提高防止确定密钥的安全性的本方法的具体实施方式中,

[0033] - 在计算步骤中对明文的至少一个子明文和密钥的至少一个子密钥应用加密算法的至少一部分,从而计算出加密结果,该结果被作为密文提供或至少被作为可以通过其它计算步骤计算出该密文的中间结果提供,其中

[0034] - 这样选择该密钥,使得其对于每一个子明文的每一个子密钥都具有相应预定次数的冲突,其中从可能冲突次数的预定集合中确定用于每个子密钥的次数。

[0035] 在该第一变形中,通过只允许这样的密钥,其中与为了用该密钥或子密钥进行加密而将哪些明文或子明文引入加密算法无关地而只能出现预定次数的冲突,使得在保持用户友好性的同时实现了本发明方法的特别的安全性。换句话说,就冲突来说只允许安全的密钥并排除采用不安全的密钥。

[0036] 在根据本发明的第二变形用于提高防止确定密钥的安全性的方法的具体实施方式中,

[0037] - 实施检查步骤,其中对明文进行检查,看其是否根据预定的一致判断准则与测试明文一致,以及

[0038] - 如果在该检查步骤中确定相应的一致,则将计数器的值增一,以及

[0039] - 只要计数器的值小于预定的最高次数值,就在计算步骤中对明文或至少明文的一部分以及密钥或至少密钥的一部分应用加密算法的至少一部分,从而计算出加密结果,该结果被作为密文提供或至少作为可以通过其它计算步骤计算出密文的中间结果提供。

[0040] 在本发明方法的第二变形中,通过分析引入加密算法中的明文,并且如果明文不只是零星或随机分布的、而是根据预定准则具有不安全的分级的特性,则进行闭锁,该闭锁是指实施本方法或至少应用由实施该方法产生的加密结果遭到拒绝,由此本方法在达到用户友好性的同时取得了特别的安全性能。

[0041] 在第一变形中的冲突可以通过所有密钥而在所有明文之间产生的冲突,也就是说子明文可以与整个明文相同,而子密钥与整个密钥相同。优选地,冲突是通过子密钥在子明文之间引起的冲突。有利的还有,密钥具有多个子密钥,而相应的明文具有相应的多个子

明文。

[0042] 根据第一变形的第一实施方式,只允许没有冲突的密钥。同其它实施方式和变形一样,在此冲突也意味着由整个密钥或由该密钥中包含的子密钥引起的整个明文之间或子明文之间的冲突。

[0043] 在本方法的第一变形的第一实施方式中尤其具有优点的是,在实施该方法时不出现冲突。因此本方法没有为试图读出密钥的攻击提供通过冲突进行攻击的可能性。

[0044] 在本方法的其它实施方式中,可以这样选择密钥,使得例如最多仅出现两次冲突,或者最多出现一次冲突,或者出现一次或两次冲突,或者出现两次或四次冲突,等等。这些实施方式的优点尤其在于,冲突的次数不是很多。冲突出现得越少,通过冲突进行攻击就越难。因此极度加大了通过冲突进行攻击的难度。

[0045] 根据第一变形的其它实施方式,一个子密钥具有至少一次冲突。优选地,子密钥也同时具有最高预定次数的冲突。

[0046] 在出现至少一次冲突的情况下,本发明的方法优选还具有另一个安全性特征。该安全性特征是,在采用加密算法之前检查子明文是否属于一个冲突的子明文对,对于该子明文对至少有一个子密钥具有至少一次冲突。换句话说,就是检查用特殊采用的加密算法和特殊采用的子密钥是否出现至少一次冲突,是出现在加密算法的结尾,还是在一个任意的中间结果中,是在总明文之间还是在子明文之间。对于采用的加密算法和子密钥至少具有一次冲突的子明文被预先标记为已索引的子明文(所谓的“索引质询”(indexed challenges))。在此再次指出,在本申请的标记方式中,作为子明文的特殊情况是通过该子明文就己能构成整个明文,作为子密钥的特殊情况是通过该子密钥就可以形成整个密钥。加密算法和子密钥的每个组合在此都具有其自身的索引的子明文组。如果检查给出该子明文属于一个这样的冲突的子明文对,则基于该检查而对于该冲突子明文对中的两个子明文的至少之一,防止将采用利用子密钥和来自该冲突对的子明文的加密算法而获得的加密结果作为密文或中间结果提供。

[0047] 通过防止将获得的加密结果提供为密文或中间结果,使得在该方法中出现的冲突对外不是可见的,而是对潜在的攻击者隐藏了的。因此尽管出现了冲突,攻击者也不能从该冲突中获得关于密钥的信息。

[0048] 如果在要分别嵌入到一个更大的整体明文中的真正的子明文之间出现相应的冲突,则优选与检查该更大的、内嵌了这些子明文的整体明文一起来检查相应的子明文。实际上,优选这样来进行该检查,使得存在已索引的子明文(索引的质询),由该子明文识别出其与所采用的密钥具有至少一个冲突。对传递到加密算法中的整个明文检查其是否含有已索引的子明文。如果含有,则如上所述对该索引的子明文阻止继续采用加密结果。

[0049] 对于所述的防止提供加密结果,可以尽管至少部分执行加密算法,但不将加密结果提供为密文或中间结果。或者,根本不执行加密算法,或者如果一个或多个真正的子明文内嵌到一个整体明文中,则至少对产生冲突的子明文不采用加密算法。

[0050] 可以对于来自一个冲突子明文对的两个子明文都防止将加密结果提供为密文或中间结果。但是,一般只对两个子明文之一实施就足以,因为相应的两个密文或中间结果通常(除了极少数例外情况)是不同的。根据“普通的”加密过程,对于来自冲突子明文对的两个子明文中的另一个,可以将通过对子密钥和子明文采用加密算法计算出的加密结果提

供为密文或中间结果。

[0051] 可以对冲突对中的至少一个子明文,不提供加密结果,而提供证明文本(Alibitext)作为密文或中间结果。

[0052] 所述证明文本例如可以通过用一个与密钥或子密钥不同的证明密钥或证明子密钥对明文或子明文采用加密算法而计算出来。

[0053] 或者,所述证明文本还可以通过对明文或子明文采用与加密算法不同的证明算法计算出来。

[0054] 或者,还可以对所述证明文本预先给定一个固定值或一个例如通过随机数发生器产生的随机值。

[0055] 如果提供了证明文本,则优选这样实施,该证明文本对攻击者来说在外部、尤其是在维护密文或中间结果时是无法识别的。为此,可从外部察觉的、根据上述一个变形提供证明文本的方法过程优选与不提供证明文本的方法过程相同,或只是不明显的不同。这可通过仅在经过一个合适测定的预定证明时间间隔之后才提供证明文本来实现。有利的是,证明时间间隔尤其是根据其持续时间和时间位置这样设置,证明文本的提供基本上与应用和至少部分运行加密算法持续得一样长,加密算法的结果根据检查由提供证明文本来代替。由此可以在期待时刻输出密文或中间结果,而不取决于其中是采用加密结果还是证明文本。

[0056] 有利的是,如果将证明文本提供为密文或中间结果,则仍然执行加密算法。有利的是,在此用错误的密钥计算错误的密文或错误的中间结果。由此在执行加密算法时出现的电流消耗也通过提供证明文本而不会发生改变或明显的改变。由此防止了攻击者成功地执行其中从运行加密算法时的电流消耗中获得关于密钥的信息的加密算法。因为这样的攻击者只有在电流消耗被明显改变的时候才能获得成功。

[0057] 在利用错误的密钥进行计算的优选实施方式中,加密算法优选在证明时间间隔内运行,并且由于该运行一般与利用正确密钥的正规运行持续得一样长,因此通常该加密算法大约一直运行到该证明时间间隔结束时才算出密文或中间结果。在该变形中,当加密算法结束了利用证明密钥的计算,也就是用证明密钥设置了“错误的”证明加密结果之后,优选证明时间间隔结束,因为用证明密钥的计算和用正确密钥的计算通常持续时间相同。其优点是,不需要额外的电路装置来测量和保持证明时间间隔。在其它变形中,为了测量和保持该证明时间间隔可以设置合适的时间发生器,例如脉冲装置。

[0058] 根据本发明的实施方式的变形,密钥分为多个子密钥,明文分为多个子明文。在此,从一个子密钥和一个子明文中计算出一个子中间结果,对于一个预定的子密钥和至少一对子明文出现预定数量的冲突。例如,对一个 16 字节长的密钥中的两字节长的子密钥出现预定数量的冲突,对于一个 16 字节长的明文中的两字节长的子明文也是如此。

[0059] 根据第二变形的第一实施方式,明文具有至少一个子明文,测试明文具有至少一个子测试明文。在此,根据预定的一致性判断准则,如果明文和测试明文的不同之处最多在于该子明文与该子测试明文相互不同并且除此之外相互一致,则在这种情况下确定一致。

[0060] 特别是,在第二变形中,明文可以具有内部数量的子明文,测试明文可以具有内部数量的子测试明文。在此,根据预定的一致性准则,如果明文和测试明文的不同之处最多在于一个子明文与一个子测试明文相互不同而除此之外相互一致,则在这种情况下确定为一

致。

[0061] 特别是,每个子明文和每个子测试明文都是两字节长。在这种情况下,根据预定的一致性判断准则,如果明文和测试明文最多有两个字节相互不同,则在这种情况下确定为一致。

[0062] 根据第二变形的另一个实施方式,用多个测试明文实施多个检查步骤。

[0063] 通过采用多个测试明文并将明文与这些测试明文进行比较,本方法实现了更高的可靠性,因为识别了更多的一致性。

[0064] 在第二变形中,计数器尤其是在根据预定的判断准则确定检查步骤的至少一部分、确切地说是多个检查步骤的部分检查步骤一致时才增一。也就是说例如 30 个检查步骤中有 5 个一致。或者,计数器还可以在根据预定的判断准则确定至少一个先前执行的检查步骤一致时才增一。

[0065] 根据第二变形的另一个实施方式,在检查步骤之前用测试明文执行至少一个先前的计算步骤,其中在该计算步骤中对该测试明文或该测试明文的至少一部分以及密钥或密钥的至少一部分应用加密算法的至少一部分。由此计算出测试加密结果。该测试明文在该计算步骤之后作为测试明文提供给检查步骤。换句话说,与明文进行比较的测试明文是来自一个先前计算步骤的明文,在该计算步骤之后存储该明文。在下一个计算步骤之前检查现在将用于加密的明文是否与上次涉及的明文一致或相似。如果两个明文只有微小的差异,则可以推断对加密算法正在实施攻击。

[0066] 根据第二变形的另一个实施方式,在用明文或至少一个子明文执行了计算步骤之后将该明文作为后续测试明文提供给后面进行的其它检查步骤。换句话说,当前加密的明文在加密后被存储起来。在下次加密时检查,用于该加密的新涉及的明文是否与上次涉及的明文一致或相似。如果两个明文只有微小的差异,则可以推断对加密算法正在实施攻击。

[0067] 根据第二变形的另一个实施方式,用后续测试明文来替换已经用于检查步骤和/或已在该检查步骤中使用的待剔除的测试明文,其中该待剔除的测试明文在随后的一个检查步骤中不作为用于执行检查步骤的测试明文。也就是说,正在加密的明文在加密后作为测试明文,并为此排除其他的测试明文。

[0068] 根据第二变形的另一个实施方式,用多个测试明文执行多个先前的计算步骤,其中对测试明文或至少一个子测试明文以及密钥或至少一个子密钥分别应用加密算法的至少一部分,从而计算出多个测试加密结果。在该实施方式中,每个测试明文在相应的在前计算步骤之后用于至少一个检查步骤。多个在前计算步骤优选连续执行。优选的,在每个计算步骤之后又执行一个检查步骤。优选的,在每个计算步骤之后将正在加密的明文作为测试明文提供给一个或多个随后进行的检查步骤。

[0069] 更为有利的是,对于新采用的测试明文分别剔除一个旧测试明文。优选的,将直接在一个计算步骤之前以及为该计算步骤采用的测试明文的数量保持恒定。

[0070] 特别是,将来自多个测试明文中的、在多个检查步骤中作为测试明文采用次数最多的测试明文作为待剔除的测试明文替换掉。

[0071] 或者,将来自多个测试明文中的、最早用作后续测试明文、尤其是从明文转换为测试明文的测试明文作为待剔除的测试明文替换掉。

[0072] 根据第二变形的实施方式,最大计数值是 1。在此,作为计数器尤其是可以采用比较单元,用于在确定一致的情况下防止将加密结果提供为密文或中间结果。

[0073] 根据第二变形的替换实施方式,最大计数值是 12。

[0074] 根据第二变形的另一实施方式,当计数器的值达到或超过预定的最大计数值时,不提供加密结果而提供证明文本作为密文或中间结果。

[0075] 由此,根据本发明被发现的攻击者不会发觉这一点,因为他在得到对他输入来加密的明文的响应时获得密文或中间结果。

[0076] 下面的实施方式既适用于本方法的第一变形又适用于本方法的第二变形。

[0077] 本发明的密钥尤其可以是二进制或十六进制编码的密钥。

[0078] 如上所述,根据本发明,尤其是可以将密钥分为多个子密钥,将明文分为多个子明文。

[0079] 根据本发明,每个子密钥都可以由两个底层子密钥(例如密钥字节)组成,每个子明文都可以由两个底层子明文(例如明文字节)组成。在此,每个底层子密钥和每个底层子明文分别为一个字节长。在这种情况下每个子密钥形成一个总共两个字节长的密钥字节对,每个子明文形成一个总共两个字节长的明文字节对。

[0080] 根据本发明,加密算法尤其可以是对称加密算法。根据本发明,加密算法尤其可以是具有密钥的哈希函数(加密的哈希函数)。

[0081] 加密算法还可以具有 8 次循环。此外根据本发明,加密算法的每次循环都具有 5 次子循环。至少有一次循环可以具有至少两次子循环。此外,每次循环可以具有 5 次子循环。

[0082] 在本发明方法的第一变形中,优选在第二次子循环之后出现预定数量或最高次数的冲突,即所谓的 2R 冲突。尤其是,例如可以这样选择密钥,使得不出现 2R 冲突。或者这样选择密钥,使得最多出现一个 2R 冲突,为此选择适当索引的明文,使得不能从外部识别 2R 冲突。外部的无法识别性可以出现在该同一个子循环之后,或者出现在随后的一个子循环之后。对于例如在第二次子循环之后出现的冲突,该冲突的不可识别性可以例如在第二次、第三次、第四次或第五次子循环之后的中间结果中产生,或在最后结果中、也就是在完成的密文中产生。

[0083] 或者,可以这样选择密钥,使得在较高级的子循环中(例如第三次循环)没有冲突,而在较低级的循环中(例如第一次和第二次循环)通过索引的明文截获可能的冲突。

[0084] 根据本发明的优选实施方式,对于第一变形和第二变形,加密算法都是 COMP128-1 算法,其具有 8 次循环,每次循环具有 5 次子循环。COMP128-1 算法尤其是作为验证算法用于根据 GSM 标准的移动无线应用,为此优选实施在 SIM 卡中。

[0085] 根据本发明的方法优选用于防止试图通过重复执行加密算法确定密钥或子密钥的攻击。在这种攻击中,优选不同的明文重复执行加密算法。通过分析输入数据,并根据该分析对密钥和明文应用加密算法来计算密文(或在密文计算路径上的中间结果),可以截获和分离出(也就是根据该分析处理)重要的输入数据。

[0086] 在此,可以通过选择没有冲突的密钥,来预先防止出现输入数据的关键组合。

[0087] 或者,如果攻击者输入输入数据的关键组合,则防止该攻击者知道他输入的输入数据是关键数据。

[0088] 在两种情况下,都对攻击者隐瞒了他可以从中确定密钥的信息。由此,利用该应用,防止了试图通过重复执行加密算法确定密钥或子密钥的攻击取得成功。

[0089] 攻击的防止可以这样来得到支持,即另外对重复执行该算法的次数计数,并在达到执行该加密算法的预定最高次数之后将后续的执行闭锁到至少预定的等待时间间隔过去之后。在此,仅当执行的预定最高次数出现在一个预定的时间间隔内时才执行该闭锁。

[0090] 执行的预定最高次数优选在 20000 到 200000 的范围内,优选大约为 65535 次,也就是 $2^{16}-1$ 。

[0091] 本发明的数据载体优选具有存储密钥的密钥存储装置,在该数据载体中实现本发明的方法或应用。在本发明方法的第一变形中,这是具有预定次数冲突的有针对选择的密钥。有利的是,对于本发明的数据载体,在密钥存储装置中还存储了证明密钥,其根据本发明可以用作证明密钥。

[0092] 可选的,对于具有至少一次冲突的密钥,本发明的数据载体可以具有明文存储装置,其中针对该密钥,对于至少一对冲突的明文或子明文存储两个明文或子明文中至少一个。优选的,对于每对冲突的明文都存储来自该对冲突明文的两个明文之一。或者还可以存储两个明文。

[0093] 可选的,如果在数据载体中实现根据本发明方法第二变形的的方法,则该数据载体还具有测试明文存储装置,其中存储至少一个测试明文或至少一个测试子明文。在此,测试明文存储装置例如具有一个按照 FIFO(先进先出)原理工作的存储器。在该情况下,在本发明的方法中,根据第二变形优选将在计算步骤中处理的明文作为后续的测试明文存入存储装置中。为此,将首先存储在存储器中的测试明文(先进先出)从该存储器中删除。在此存储器中元素的数量保持恒定。

[0094] 优选地,在数据载体中还至少部分地实现移动电话卡的功能。在这种情况下,数据载体优选是 SIM 卡,其中可选地利用本发明的应用实现本发明的方法。

[0095] 在本发明的数据载体中,优选在定制该数据载体时将密钥存储在数据载体中,在此,这样选择密钥,使得该密钥的每个子密钥对每个子明文都具有相应预定数量的冲突,其中对于每个子密钥的次数由预定的可能冲突集合确定。

[0096] 可选地,如果至少一个子密钥具有至少一次冲突,则在定制数据载体时除了该密钥之外还在数据载体中存储对应该密钥的冲突明文或子明文。优选地,对每对冲突的(子)明文只存储一个(子)明文,或者存储两个(子)明文。

[0097] 此外,在定制时还在数据载体中这样存储一个证明密钥,使得在基于检查和分析明文而因为即将发生冲突没有采用正确密钥时,加密算法采用该证明密钥。

附图说明

[0098] 下面借助加密算法 Comp128-1 的实施例和参考附图详细解释本发明。

[0099] 图 1 部分地示出 Comp128-1 算法的一次循环的第一两重子循环的示意图;

[0100] 图 2 示出一个表,其中示出从总共 65536 个可能的密钥字节对中有多少个密钥字节对(右栏)在第二子循环的末尾具有预定的 n 次冲突(左栏);

[0101] 图 3 示出一个表,其包括一个具有特定值的 16 字节长的密钥 K_i 的所有密钥字节对 (KA_1, KA_2),和对应的最多具有一次冲突的冲突明文字节对 (CA_{1_1}, CA_{2_1}) 和 (CA_{1_2}, CA_{2_2});

在此两个明文字节对 $(CA1_1, CA2_1)$ 和 $(CA1_2, CA2_2)$ 中有一个被随机选中并写在卡上,在该例中是黑体印刷的明文字节对;

[0102] 图 4a, 4b 示出对 5 个不同明文的子明文(明文字节对)与图 3 的密钥 K_i 冲突进行检查的质询 1、质询 2、质询 3、质询 4、质询 5。

具体实施方式

[0103] 图 1 示出 Comp128-1 算法的一次子循环的第一两重子循环的部分示意图。在该算法中,由一个 16 字节长并具有 16 个密钥字节 $K[0], K[1], \dots, K[15]$ 的密钥 K_i 以及一个 16 字节长并具有 16 个明文字节 $C[0], C[1], \dots, C[15]$ 的明文 C (质询)计算出一个 12 字节长的哈希值。

[0104] 在第一子循环中,对于 $i = 0 \dots 7$ 分别计算第 i 个密钥字节 $K[i]$ 和第 i 个明文字节 $C[i]$,以及第 $(i+8)$ 个密钥字节 $K[i+8]$ 和第 $(i+8)$ 个明文字节 $C[i+8]$,从而对于从 0 到 7 的每个 i 来说分别计算第一次子循环 $U1, U2, U3, U4$ 的 4 个结果。由 $U1$ 和 $U2$ 计算第二次子循环的第一结果 $Z1$ 和第二次子循环的第二结果 $Z2$ 。由 $U3$ 和 $U4$ 计算第二次子循环的第三结果 $Z3$ 和第二次子循环的第四结果 $Z4$ 。对于 $i = 0$,第二次子循环的结果 $Z1, Z2, Z3, Z4$ 只与具有两个密钥字节 $K[0]$ 和 $K[8]$ 的密钥字节对 $(KA1, KA2)$ 和具有两个明文字节 $C[0]$ 和 $C[8]$ 的明文字节对有关,但与其他密钥字节和明文字节无关。第二次子循环的结果 $Z1, Z2, Z3, Z4$ 因此只分别与两个密钥字节和两个明文字节有关。

[0105] Comp128-1 的第一次子循环这样构成,没有冲突出现。相反,在随后的子循环中出现冲突。第 n 次子循环之后的冲突在此也称为 nR 冲突。如果在第二次子循环之后对于 $2R$ 结果 $Z1, Z2, Z3, Z4$ 而言在明文字节 $C[0]$ 和 $C[8]$ 之间出现冲突,即 $2R$ 冲突,也就是说如果存在明文字节对 $(CA1, CA2) = (C[0], C[8])$ 的两个不同值,即提供相同 $2R$ 结果 $Z1, Z2, Z3, Z4$ 的 $(CA1_1, CA2_1)$ 和 $(CA1_2, CA2_2)$,则可以从中确定对应密钥字节对 $(KA1, KA2) = (K[0], K[8])$ 的两个密钥字节 $K[0]$ 和 $K[8]$,因为结果 $Z1, Z2, Z3, Z4$ 只与两个密钥字节有关。为此针对明文字节对 $(CA1, CA2) = (C[0], C[8])$ 用所有可能的密钥字节对 $(KA1, KA2) = (K[0], K[8])$ 计算该算法的第一两重子循环,并由此针对每个可能的密钥字节对 $(KA1, KA2) = (K[0], K[8])$ 计算一个 $2R$ 结果。可能的密钥字节对的数量是 2^{16} ,也就是 65536。因此,对每个明文字节对计算 65536 个 $2R$ 结果,对这些结果检查 $Z1, Z2, Z3, Z4$ 中的冲突。 $2R$ 结果和冲突的 $2R$ 结果一致的密钥字节对是要查找的产生冲突的密钥字节对。根据通过这种方式确定的密钥字节对,可以确定 16 字节密钥的其余 14 个密钥字节。

[0106] 因此,如果根据本发明第一变形的实施方式将具有冲突的密钥从该应用中排除出去,则不能通过 $2R$ 冲突的方式确定密钥。但是由此极大地限制了所有可用密钥的密钥空间,也就是对每个密钥字节对 $(KA1, KA2) = (K[i], K[i+8])$ 限制为总共 65536 个可能的密钥字节对中的 769 个,如图 2 所示。因此整个密钥空间从 2^{128} 减小到 $2^{76.7}$ 。

[0107] 图 2 示出一个表,其中示出从总共 65536 个可能的密钥字节对中有多少个密钥字节对(右栏)在第二次子循环的末尾具有预定的 n 次冲突(左栏)。该表通过用所有可能的密钥字节对 $(KA1, KA2)$ 计算所有可能的明文字节对 $(CA1, CA2)$ 产生。该表示出,65536 个可能的密钥字节对中有 769 个密钥字节对没有冲突。该表还示出,65536 个可能的密钥字节对中有 3301 个密钥字节对只有一个冲突,也就是只有一对冲突的密钥字节对,即 $(CA1_1,$

CA2₁) 和 (CA1₂, CA2₂), 其在第二次循环中提供相同的结果。7166 个密钥字节对具有两个冲突, 也就是存在两对冲突的密钥字节对, 即第一对 [(CA1₁, CA2₁)₁, (CA1₂, CA2₂)₁] 和第二对 [(CA1₁, CA2₁)₂, (CA1₂, CA2₂)₂]。11001 个密钥字节对具有 3 个冲突, 也就是还存在第三冲突对 [(CA1₁, CA2₁)₃, (CA1₂, CA2₂)₃], 等等。如果因此对于密钥的子密钥来说, 也就是对于各个密钥字节对 (KA1, KA2) = (K[i], K[i+8]) 不是允许 0 次而是允许最多 3 个冲突, 则针对每个密钥字节对的密钥空间都包含 22237 个容许的密钥字节对, 也就是大约是允许 0 次冲突时的 3 倍。对于最多一个容许冲突, 总是还存在 4070 个容许的密钥字节对, 并因此存在有 2^{95.9} 个密钥的总密钥空间。

[0108] 图 3 示出一个表, 包括一个具有特定值的 16 字节长的 GSM 认证密钥 Ki 的所有密钥字节对 (KA1, KA2), 和对应的最多具有一次冲突的冲突明文字节对 (CA1₁, CA2₁) 和 (CA1₂, CA2₂)。密钥 Ki 在所示例中具有值 eb b5 85 b7 03 ac8a 35 c1 cc 04 5a cf e1 d9 b2, 并存储在移动电话的 SIM 卡中。这样选择密钥, 使得其子密钥最多具有一次冲突。表的左栏示出密钥字节对 (KA1, KA2) = (K[i], K[i+8]), i = 0...7。表的右栏示出对应的冲突的明文字节对。也就是说, 在表中示出的例子中, 8 个密钥字节对 (子密钥) 中有 3 个没有冲突。对于这些密钥字节对没有列出明文字节对。8 个密钥字节对中有 5 个只有一个冲突。对于这些密钥字节对, 右栏只包含了一对冲突的明文字节对。例如包含第一明文对 (CA1₁, CA2₁) = (59 a8) 和第二明文对 (CA1₂, CA2₂) = (af b1) 的该对 (59a8/afb1) 与密钥字节对 (KA1, KA2) = (b5cc) 恰好产生一个冲突。

[0109] 在定制 SIM 卡时, 将包含列在左栏中的密钥字节对 (KA1, KA2) 和列在右栏中的对应冲突明文字节对 (CA1₁, CA2₁) 和 (CA1₂, CA2₂) 的该表 (或该表的一部分) 存储在 SIM 卡中。优选的, 在定制 SIM 卡时, 从每一对冲突的冲突明文字节对 (CA1₁, CA2₁) 和 (CA1₂, CA2₂) 的右栏中只将两个明文字节对之一存储在 SIM 卡中, 因为这足以使本方法生效, 此外还节省了存储器。优选的, 随机挑选出待存储的两个明文字节对 (CA1₁, CA2₁) 和 (CA1₂, CA2₂), 然后写在卡上。在图 3 的表中, 在定制时相应存储在卡上的明文字节对以黑体印刷。

[0110] 如果在图 3 的例中这样选择密钥 Ki, 使得其子密钥最多具有 n 个冲突, 则在图 3 表的右栏中存在最多包含 n 对明文字节对 (CA1₁, CA2₁), (CA1₂, CA2₂)... (CA1_n, CA2_n) 的行。

[0111] 对于图 3 的例子的对应转换, 其中这样选择密钥 Ki, 使得其子密钥最多具有 n 个冲突, 针对左栏中的一个子密钥, 与图 3 类似的表的行在右栏中最多包含 n 对明文字节对 (CA1₁, CA2₁), (CA1₂, CA2₂)... (CA1_n, CA2_n)。

[0112] 如果在用具有图 3 例子中的值的密钥 Ki 定制的 SIM 卡中输入一个明文, 则检查该明文是否在各个字节对位置 (CA1, CA2) 分别具有一个等于来自一对冲突的明文字节对中的一个明文字节对的值。图 4a 和图 4b 中示出针对冲突的明文字节对来检查明文。

[0113] 图 4a, 4b 示出对 5 个不同明文检查其子明文 (明文字节对) 与图 3 的密钥 Ki 的冲突的质询 1、质询 2、质询 3、质询 4、质询 5。

[0114] 图 4a 示出采用的 5 个明文质询 1、质询 2、质询 3、质询 4、质询 5 的值。

[0115] 图 4b 示出图 4a 的 5 个明文质询 i, i = 1, 2, 3, 4, 5 分为明文字节对 (子明文) 的值。对于每个明文, 分别对每个明文字节对检查其是否属于一对冲突的明文字节对。对该检查采用图 3 的表。如果根据图 3 的表, 对于一个明文质询 i 来说没有检查的明文字节对属于一对冲突的明文字节对, 则执行包含图 3 的正确密钥 Ki 的验证算法 Comp128-1。对

于明文质询 1、2、4、5 也是如此。相反,对于明文质询 3,在位置 ($K[6]$, $K[14]$) 处的明文字节对 ($84\ 4a$) 与明文字节对 ($CA1_i$, $CA2_i$) = ($84\ 4a$) 相同,后者与密钥 K_i 的两个密钥字节 ($K[6]$, $K[14]$) = ($8ad9$) 产生冲突 (图 3 表中的倒数第二行)。因此,对于明文质询 3,验证算法 Comp128-1 不是利用图 3 的正确密钥 K_i 执行,而是利用同样在定制时存储在 SIM 卡中的证明密钥执行。由此,对于明文质询 3 来说计算出一个错误的密文。因此,由于冲突而实际上相同的密文通过采用证明密钥而不同,因此冲突对外是不可识别的。此外,因为除了采用错误的密钥之外正规执行验证算法,因此既不能由电流消耗又不能由 SIM 卡的时间响应来识别出已经处理了冲突的明文。因此,攻击者在运用算法时也不能从电流和时间曲线中通过冲突推断出密钥,即使出现了冲突。

[0116] 根据本发明的方法和应用还可以采用任意其它加密算法。尤其是可以采用各种具有至少两次子循环的任意加密算法,尤其是这样的加密算法,其中从至少两次子循环中计算出中间结果作为一次预定子循环的结果,从而在预定子循环之后出现预定次数的冲突。尤其是,可以采用其中在第二次子循环之后出现预定次数的冲突的任意加密算法。

[0117] 对于本发明数据载体的任意一个实施方式,在此都可以确定,在本专利文献中的实现可以按照软件形式、硬件形式或混合的硬件 - 软件形式实现。

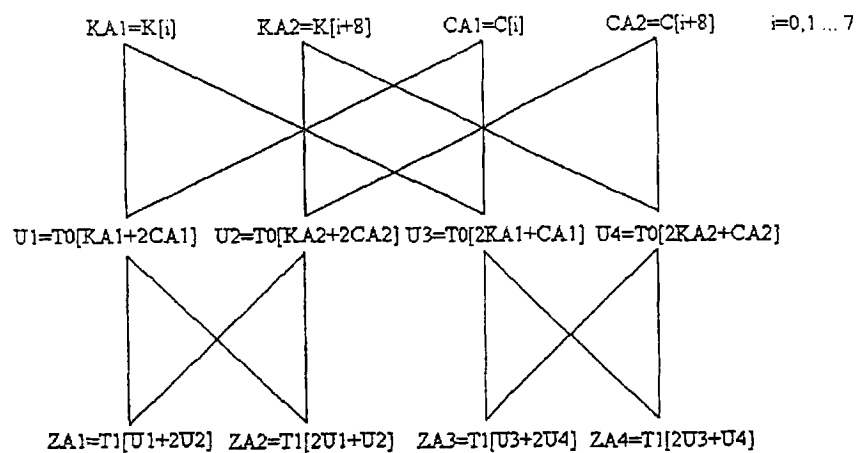


图 1

$Ki = eb\ b5\ 85\ b7\ 03\ ac\ 8a\ 35\ c1\ cc\ 04\ 5a\ cf\ e1\ d9\ b2$

密钥字节对 KA1 KA2	明文字节对 CA1, CA2, 和 CA1, CA2 的冲突对
eb c1	-
b5 cc	59 a8 af b1
85 04	93 0a ea e5
b7 5a	-
03 cf	-
ac e1	0a 2f 42 2f
8a d9	84 4a d9 8b
35 b2	19 77 f4 c7

图 3

明文对之间的冲突次数n (CA1i, CA2i), i=1...n	具有n次冲突的密钥字节对的个数 KA1 KA2
0	769
1	3301
2	7166
3	11001
4	12690
5	11238
6	8305
7	5289
8	3103
9	1511
10	733
11	283
12	105
13	35
14	1
15	3
16	2
17	1

图 2

质询 1: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

质询 2: f4 a3 40 21 33 81 c9 ff c7 b8 98 76 56 ab d5 55

质询 3: 12 db 3f 00 f3 6f 84 d9 cd e4 a0 3a 45 b6 4a 8b

质询 4: 54 fc 31 0b 10 aa 42 23 9a fd 09 f1 9a d4 2f 45

质询 5: 91 af 32 ea 1a 89 d4 12 34 b1 1a e5 aa bd 56 34

图 4a

质询1	质询2	质询3	质询4	质询5
00 88	f4 c7	12 cd	54 9a	91 34
11 99	a3 b8	db e4	fc fd	af b1
22 aa	40 98	3f a0	31 09	32 1a
33 bb	21 76	00 3a	0b f1	ea e5
44 cc	33 56	f3 45	10 9a	1a aa
55 dd	81 ab	6f b6	aa d4	89 bd
66 ee	c9 d5	84 4a	42 2f	d4 56
77 ff	ff 55	d9 8b	23 45	12 34
正确结果	正确结果	错误结果	正确结果	正确结果

图 4b