(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105940439 B
(45)授权公告日 2020.01.17

(21)申请号 201580006205.3
(22)申请日 2015.02.03
(65)同一申请的已公布的文献号
申请公布号 CN 105940439 A
(43)申请公布日 2016.09.14
(30)优先权数据
14/171,558 2014.02.03 US
(85)PCT国际申请进入国家阶段日
2016.07.28
(86)PCT国际申请的申请数据
PCT/US2015/014294 2015.02.03
(87)PCT国际申请的公布数据
WO2015/117144 EN 2015.08.06
(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州
(72)发明人 郭晓飞 郭旭 B•B•布伦利
(74)专利代理机构 北京律盟知识产权代理有限责任公司 11287
代理人 宋献涛
(51)Int.Cl.
*G09C 1/00*(2006.01)
*H04L 9/00*(2006.01)
*H04L 9/06*(2006.01)
(56)对比文件
EP 1722502 A1,2006.11.15,
US 2010232602 A1,2010.09.16,
US 2006171532 A1,2006.08.03,
US 2002/0051534 A1,2002.05.02,
CN 1656733 A,2005.08.17,
审查员 刘燕

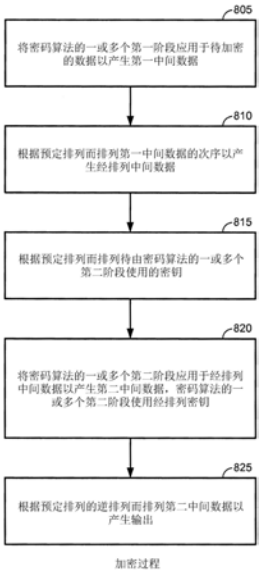
权利要求书5页 说明书12页 附图9页

(54)发明名称

使用排列应对对密码算法的旁通道攻击的对策

(57)摘要

本发明提供可用以帮助防止对密码算法的旁通道攻击的用于加密数据的技术。根据这些技术的实例方法包含根据预定排列而排列第一中间数据的次序以产生经排列中间数据。所述第一中间数据由密码算法的一或多个第一阶段输出。所述方法还包含:根据所述预定排列而排列待由密码算法的一或多个第二阶段使用的密钥;将密码算法的所述一或多个第二阶段应用于所述经排列中间数据以产生第二中间数据,所述密码算法的所述一或多个第二阶段使用所述经排列密钥;以及根据所述预定排列的逆排列而排列所述第二中间数据以产生输出。



加密过程

CN 105940439 B

1.一种用于在计算装置上加密数据的方法,所述方法包括:

从所述计算装置上的应用接收数据;

在执行加密时通过所述计算装置的一个或多个处理组件使用随机化功率消耗的技术来加密所述数据,通过以下步骤来执行所述加密:

对于密码算法的每一轮,通过从多个字节次序排列中选择排列来确定所选排列;

根据所述所选排列而排列第一中间数据的字节的次序以产生经排列中间数据,所述第一中间数据由所述密码算法的所述轮的一或多个第一阶段输出;

根据所述所选排列而排列待由所述密码算法的一或多个第二阶段使用的密钥的字节的次序,使得所述密钥的所述次序以及所述第一中间数据的所述次序由相同的排列函数确定;

将所述密码算法的所述一或多个第二阶段应用于所述经排列中间数据以产生第二中间数据,所述密码算法的所述一或多个第二阶段使用所述经排列密钥,在应用所述密码算法的所述一或多个第二阶段时,对所述第一中间数据以及所述密钥的所述次序进行的排列将随机性引入所述一个或多个处理组件的所述功率消耗;以及

根据所述所选排列的逆排列而排列所述第二中间数据以产生密文输出;

将所述密文输出存储在所述计算装置的存储器中;

解密所述密文输出以产生解密数据;以及

将所述解密数据提供给所述应用。

2.根据权利要求1所述的方法,其进一步包括:

将所述密码算法的所述一或多个第一阶段应用于待加密的数据以产生所述第一中间数据。

3.根据权利要求1所述的方法,其进一步包括:

从一组排列选择排列,其中根据所述所选排列而排列所述第一中间数据的所述次序以产生经排列中间数据包括:使用所述所选排列来排列所述第一中间数据的所述次序。

4.根据权利要求3所述的方法,其中从所述组排列选择所述排列包括:

产生随机数种子值;以及

基于所述随机数种子值而从所述组排列选择所述排列。

5.根据权利要求3所述的方法,其中从所述组排列选择所述排列包括:

基于所选模式而从所述组排列选择所述排列。

6.根据权利要求3所述的方法,其中根据所述所选排列的所述逆排列而排列所述第二中间数据以产生所述输出包括:基于来自所述组排列的所述所选排列而从一组逆排列选择所述逆排列。

7.根据权利要求1所述的方法,其中所述密码算法为高级加密标准AES算法,且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮,且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮;或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮,且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

8.一种用于在计算装置上加密数据的系统,所述系统包括:

用于从所述计算装置上的应用接收数据的装置;

用于在执行加密时通过所述计算装置的一个或多个处理组件使用随机化功率消耗的技术来加密所述数据的装置，用于加密所述数据的装置包括：

用于对于密码算法的每一轮，通过从多个字节次序排列中选择排列来确定所选排列的装置；

用于根据所述所选排列而排列第一中间数据的字节的次序以产生经排列中间数据的装置，所述第一中间数据由所述密码算法的所述轮的一或多个第一阶段输出；

用于根据所述所选排列而排列待由密码算法的一或多个第二阶段使用的密钥的字节的次序，使得所述密钥的所述次序以及所述第一中间数据的所述次序由相同的排列函数确定的装置；

用于将所述密码算法的所述一或多个第二阶段应用于所述经排列中间数据以产生第二中间数据的装置，所述密码算法的所述一或多个第二阶段使用所述经排列密钥，在应用所述密码算法的所述一或多个第二阶段时，对所述第一中间数据以及所述密钥的所述次序进行的排列将随机性引入所述一个或多个处理组件的所述功率消耗；以及

用于根据所述所选排列的逆排列而排列所述第二中间数据以产生密文输出的装置；

用于将所述密文输出存储在所述计算装置的存储器中的装置；

用于解密所述密文输出以产生解密数据的装置；以及

用于将所述解密数据提供给所述应用的装置。

9.根据权利要求8所述的系统，其进一步包括：

用于将所述密码算法的所述一或多个第一阶段应用于待加密的数据以产生所述第一中间数据的装置。

10.根据权利要求8所述的系统，其进一步包括：

用于从一组排列选择排列的装置，且

其中所述用于根据所述所选排列而排列所述第一中间数据的所述次序以产生经排列中间数据的装置包括用于使用所述所选排列来排列所述第一中间数据的所述次序的装置。

11.根据权利要求10所述的系统，其中所述用于从所述组排列选择所述排列的装置包括：

用于产生随机数种子值的装置；以及

用于基于所述随机数种子值而从所述组排列选择所述排列的装置。

12.根据权利要求10所述的系统，其中所述用于从所述组排列选择所述排列的装置包括：

用于基于所选模式而从所述组排列选择所述排列的装置。

13.根据权利要求10所述的系统，其中所述用于根据所述所选排列的所述逆排列而排列所述第二中间数据以产生所述输出的装置包括用于基于来自所述组排列的所述所选排列而从一组逆排列选择所述逆排列的装置。

14.根据权利要求8所述的系统，其中所述密码算法为高级加密标准AES算法，且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮；或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

15.一种非暂时性计算机可读媒体，在其上存储有用于加密数据的计算机可读指令，包括经配置以致使计算机执行以下操作的指令：

从所述计算机上的应用接收数据；

在执行加密时通过所述计算机的一个或多个处理组件使用随机化功率消耗的技术来加密所述数据，其中致使所述计算机加密所述数据的指令包括经配置以致使所述计算机执行以下操作的指令：

对于密码算法的每一轮，通过从多个字节次序排列中选择排列来确定所选排列；

根据所述所选排列而排列第一中间数据的字节的次序以产生经排列中间数据，所述第一中间数据由所述密码算法的所述轮的一或多个第一阶段输出；

根据所述所选排列而排列待由所述密码算法的一或多个第二阶段使用的密钥的字节的次序，使得所述密钥的所述次序以及所述第一中间数据的所述次序由相同的排列函数确定；

将所述密码算法的所述一或多个第二阶段应用于所述经排列中间数据以产生第二中间数据，所述密码算法的所述一或多个第二阶段使用所述经排列密钥，在应用所述密码算法的所述一或多个第二阶段时，对所述第一中间数据以及所述密钥的所述次序进行的排列将随机性引入所述一个或多个处理组件的所述功率消耗；以及

根据所述所选排列的逆排列而排列所述第二中间数据以产生密文输出；

将所述密文输出存储在所述计算机的存储器中；

解密所述密文输出以产生解密数据；以及

将所述解密数据提供给所述应用。

16.根据权利要求15所述的非暂时性计算机可读媒体，其进一步包括经配置以致使所述计算机执行以下操作的指令：

将所述密码算法的所述一或多个第一阶段应用于待加密的数据以产生所述第一中间数据。

17.根据权利要求15所述的非暂时性计算机可读媒体，其进一步包括经配置以致使所述计算机执行以下操作的指令：

从一组排列选择排列，且

其中所述经配置以致使所述计算机根据所述所选排列而排列所述第一中间数据的所述次序以产生经排列中间数据的指令包括经配置以致使所述计算机使用所述所选排列来排列所述第一中间数据的所述次序的指令。

18.根据权利要求17所述的非暂时性计算机可读媒体，其中所述经配置以致使所述计算机从所述组排列选择所述排列的指令包括经配置以致使所述计算机执行以下操作的指令：

产生随机数种子值；以及

基于所述随机数种子值而从所述组排列选择所述排列。

19.根据权利要求17所述的非暂时性计算机可读媒体，其中所述经配置以致使所述计算机从所述组排列选择所述排列的指令包括经配置以致使所述计算机执行以下操作的指令：

基于所选模式而从所述组排列选择所述排列。

20.根据权利要求17所述的非暂时性计算机可读媒体，其中所述经配置以致使所述计算机根据所述所选排列的所述逆排列而排列所述第二中间数据以产生所述输出的指令包括经配置以致使所述计算机基于来自所述组排列的所述所选排列而从一组逆排列选择所述逆排列的指令。

21.根据权利要求15所述的非暂时性计算机可读媒体，其中所述密码算法为高级加密标准AES算法，且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮；或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

22.一种用于在计算装置中加密数据的电路，其包括：

第一组组件，其经配置以从所述计算装置上的应用接收数据；

第二组组件，其经配置以在执行加密时通过所述计算装置的一个或多个处理组件使用随机化功率消耗的技术来加密所述数据，其中所述第二组组件包括：

第三组组件，其经配置以根据所选排列而排列第一中间数据的字节的次序以产生经排列中间数据，所述第一中间数据由密码算法的轮的一或多个第一阶段输出，所述第三组组件经配置以对于所述密码算法的每一轮，通过从多个字节次序排列中选择排列来确定所述所选排列；

第四组组件，其经配置以根据所述所选排列而排列待由所述密码算法的一或多个第二阶段使用的密钥的字节的次序；

第五组组件，其经配置以将所述密码算法的所述一或多个第二阶段应用于所述经排列中间数据以产生第二中间数据，所述密码算法的所述一或多个第二阶段使用所述经排列密钥，在应用所述密码算法的所述一或多个第二阶段时，对所述第一中间数据以及所述密钥的所述次序进行的排列将随机性引入所述一个或多个处理组件的所述功率消耗；以及

第六组组件，其经配置以根据所述所选排列的逆排列而排列所述第二中间数据以产生密文输出；以及

第七组组件，其经配置以将所述密文输出存储在所述计算装置的存储器中，解密所述密文输出以产生解密数据，并将所述解密数据提供给所述应用。

23.根据权利要求22所述的电路，其进一步包括：

第八组组件，其经配置以将所述密码算法的所述一或多个第一阶段应用于待加密的数据以产生所述第一中间数据。

24.根据权利要求22所述的电路，其进一步包括：

第九组组件，其经配置以从一组排列选择排列，其中根据所述所选排列而排列所述第一中间数据的所述次序以产生经排列中间数据包括：使用来自所述组排列的所述所选排列来排列所述第一中间数据的所述次序。

25.根据权利要求24所述的电路，其中所述第九组组件进一步经配置以：

产生随机数种子值；以及

基于所述随机数种子值而从所述组排列选择所述排列。

26.根据权利要求24所述的电路，其中所述第九组组件进一步经配置以：

基于所选模式而从所述组排列选择所述排列。

27.根据权利要求24所述的电路，其中所述第六组组件经配置以基于所述所选排列而从一组逆排列选择所述逆排列。

28.根据权利要求22所述的电路，其中所述密码算法为高级加密标准AES算法，且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮；或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

29.根据权利要求22所述的电路，其中所述第一组组件包括多路复用器，所述多路复用器经配置以接收选择信号且经配置以基于所述选择信号确定所述所选排列。

# 使用排列应对对密码算法的旁通道攻击的对策

## 背景技术

[0001] 各种加密技术可用以防止对受保护数据的未授权的存取和/或修改。然而，一些加密技术可易受损于旁通道攻击。旁通道攻击为基于从密码系统的物理实施方案获得的信息的攻击，且通常并非对密码算法的蛮力攻击或对算法中固有的理论薄弱的攻击。旁通道攻击可用以收集关于密码算法如何操作的信息，包含密码密钥、部分状态信息、和/或关于正经加密的信息的完全或部分纯文本信息。

[0002] 功率分析和电磁(EM)攻击为可用以危害密码算法的两种类型的旁通道攻击的实例。在功率分析攻击中，攻击者监视已实施遭受攻击的密码算法的装置的功率消耗。功率分析攻击可在复杂度方面不同。简单功率分析(SPA)攻击涉及解译功率轨迹，功率轨迹为随时间推移的电活动的曲线，由实施遭受攻击的密码算法的硬件产生以便导出关于密码算法的信息。差异性功率分析(DPA)涉及更高级功率分析攻击技术，功率分析攻击技术将统计分析应用于从由遭受攻击的装置执行的多个加密操作采集的数据。统计分析可向攻击者提供可用以确定遭受攻击的密码算法内的中间值的信息。在EM攻击中，攻击者监视来自已实施密码算法的硬件的电磁发散。攻击者可分析这些发散以导出关于流经硬件的电流的信息，且使用所述信息以识别在每一时钟周期期间在装置内发生的事件。其它类型的旁通道攻击包含：差异性错误分析，其中在尝试显露关于密码算法的信息时将错误引入到加密计算中；时序攻击，其中攻击是基于当正执行密码算法时测量某些计算任务执行以来要花费多久；和声音攻击，其中攻击是基于当正执行密码算法时从实施遭受攻击的密码算法的装置的硬件发散的声音。

[0003] 许多装置，例如移动电话、平板计算机、膝上型计算机和/或其它此装置是使用基于互补金属氧化物半导体(CMOS)技术的数字电路加以建构。CMOS技术通常用于数字逻辑电路、静态随机存取存储器(SRAM)、微处理器和微控制器中。CMOS实施方案可容易遭受功率分析和EM攻击。CMOS数字电路的静态功耗通常极低。当通过不同输入对CMOS数字电路计时时，数字电路改变状态。这些状态改变引起内部电容器的充电和放电。所得电压波动取决于正计算的数据。希望破坏加密方案的恶意方可监视装置的功率消耗和/或来自装置的EM发散，以使正接收的数据与功率消耗和/或EM发散关联。分析此测试的结果可显露由加密方案使用的密钥、由密码算法产生的中间值、和/或攻击者可能够利用以危害密码算法的其它信息。

[0004] 图1说明可用以进行对密码算法的功率分析攻击的实例过程。图1中所说明的功率分析攻击利用蛮力方法以尝试确定由密码算法使用的密钥。图1中所说明的实例过程用以攻击高级加密标准(AES)算法，但类似程序可用以攻击其它类型的加密技术。为了让功率分析攻击成功，攻击者必须知晓遭受攻击的算法，以使得可制作模拟假设功率消耗的功率模型，且攻击者必须知晓电路的哪些功率轨迹与正计算的数据关联。使用此信息，攻击者可使用以下步骤对特定装置使用的密码算法进行功率分析攻击：

[0005] (1)可选择所执行密码算法的中间结果。举例来说，如果攻击者察觉特定装置已实施一版本的高级加密标准(AES)算法，则攻击者可将实施于装置上的AES算法的第一轮的输

出选择为攻击点。攻击者还可选择AES算法的其它轮。举例来说，AES算法的倒数第二轮还可由攻击者选为目标。

[0006] (2)可产生基于纯文本输入和密钥假设的假设中间值假设。举例来说，可通过向密码算法提供已知纯文本值和一组密钥假设来产生假设中间值。返回到AES实例，假设中间值可为AES算法的第一轮或攻击者已定为目标的AES算法的任一轮的输出。

[0007] (3)可接着将假设中间值映射到抽象功率消耗模型。抽象功率消耗模型是基于正遭受攻击的密码算法(阶段103)。功率消耗将根据密码算法的类型而改变且可针对密码算法的各阶段或轮而估计功率消耗。

[0008] (4)可接着在经配置以使用正遭受攻击的密码算法的真实移动装置上测量密码算法的目标阶段的功率轨迹(阶段104)。功率轨迹为随时间推移使用的电流的曲线，且功率轨迹可显露密码算法的可允许攻击者以导出密钥的各轮或阶段的属性。

[0009] (5)可接着使功率轨迹与抽象消耗模型相关以尝试识别密钥或与密码算法相关联的密钥的至少一部分(阶段105)。

## 发明内容

[0010] 根据本发明的一种用于加密数据的实例方法包含：根据预定排列而排列第一中间数据的次序以产生经排列中间数据，所述第一中间数据由密码算法的一或多个第一阶段输出。所述方法还包含根据所述预定排列而排列待由所述密码算法的一或多个第二阶段使用的密钥；将所述密码算法的所述一或多个第二阶段应用于所述经排列中间数据以产生第二中间数据，所述密码算法的所述一或多个第二阶段使用所述经排列密钥；和根据所述预定排列的逆排列而排列所述第二中间数据以产生输出。

[0011] 此方法的实施方案可包含以下特征中的一或多者。将所述密码算法的所述一或多个第一阶段应用于待加密的数据以产生所述第一中间数据。从一组排列选择排列，其中根据所述预定排列而排列所述第一中间数据的所述次序以产生经排列中间数据包括使用所述所选排列来排列所述第一中间数据的所述次序。从所述组排列选择所述排列包含产生随机数种子值，和基于所述随机数种子值而从所述组排列选择所述排列。从所述组排列选择所述排列包含基于预定模式而从所述组排列选择所述排列。根据所述预定排列的所述逆排列而排列所述第二中间数据以产生所述输出包含基于所述所选排列而从一组逆排列选择所述逆排列。所述密码算法为高级加密标准(AES)算法，且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮；或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

[0012] 根据本发明的一种用于加密数据的系统包含用于根据预定排列而排列第一中间数据的次序以产生经排列中间数据的装置，所述第一中间数据由密码算法的一或多个第一阶段输出；用于根据所述预定排列而排列待由密码算法的一或多个第二阶段使用的密钥的装置；用于将所述密码算法的所述一或多个第二阶段应用到所述经排列中间数据以产生第二中间数据的装置，所述密码算法的所述一或多个第二阶段使用所述经排列密钥；和用于根据所述预定排列的逆排列而排列所述第二中间数据以产生输出的装置。

[0013] 此系统的实施方案可包含以下特征中的一或多者。用于将所述密码算法的所述一

或多个第一阶段应用于待加密的数据以产生所述第一中间数据的装置。用于从一组排列选择排列的装置，且用于根据所述预定排列而排列所述第一中间数据的所述次序以产生经排列中间数据的所述装置包括用于使用所述所选排列来排列所述第一中间数据的所述次序的装置。用于从所述组排列选择所述排列的所述装置包含用于产生随机数种子值的装置，和用于基于所述随机数种子值而从所述组排列选择所述排列的装置。用于从所述组排列选择所述排列的所述装置包含用于产生随机数种子值的装置，和用于基于所述随机数种子值而从所述组排列选择所述排列的装置。用于根据所述预定排列的所述逆排列而排列所述第二中间数据以产生所述输出的所述装置包含用于基于所述所选排列而从一组逆排列选择所述逆排列的装置。所述密码算法为高级加密标准(AES)算法，且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮；或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

[0014] 根据本发明的一种非暂时性计算机可读媒体于其上存储有用于加密数据的计算机可读指令。所述媒体包括经配置以致使计算机执行以下操作的指令：根据预定排列而排列第一中间数据的次序以产生经排列中间数据，所述第一中间数据由密码算法的一或多个第一阶段输出；根据所述预定排列而排列待由所述密码算法的一或多个第二阶段使用的密钥；将所述密码算法的所述一或多个第二阶段应用到所述经排列中间数据以产生第二中间数据，所述密码算法的所述一或多个第二阶段使用所述经排列密钥；和根据所述预定排列的逆排列而排列所述第二中间数据以产生输出。

[0015] 此非暂时性计算机可读媒体的实施方案可包含以下特征中的一或多者。经配置以致使所述计算机将所述密码算法的所述一或多个第一阶段应用于待加密的数据以产生所述第一中间数据的指令。经配置以致使所述计算机从一组排列选择排列的指令，且经配置以致使所述计算机根据所述预定排列而排列所述第一中间数据的所述次序以产生经排列中间数据的所述指令包含经配置以致使所述计算机使用所述所选排列来排列所述第一中间数据的所述次序的指令。经配置以致使所述计算机从所述组排列选择所述排列的所述指令包含经配置以致使所述计算机执行以下操作的指令：产生随机数种子值，和基于所述随机数种子值而从所述组排列选择所述排列。经配置以致使所述计算机从所述组排列选择所述排列的所述指令包含经配置以致使所述计算机基于预定模式而从所述组排列选择所述排列的指令。经配置以致使所述计算机根据所述预定排列的所述逆排列而排列所述第二中间数据以产生所述输出的所述指令包含经配置以致使所述计算机基于所述所选排列而从一组逆排列选择所述逆排列的指令。所述密码算法为高级加密标准(AES)算法，且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮；或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

[0016] 根据本发明的一种用于加密数据的电路包含第一组组件，其经配置以根据预定排列而排列所述第一中间数据的次序以产生经排列中间数据，所述第一中间数据由密码算法的一或多个第一阶段输出；第二组组件，其经配置以根据所述预定排列而排列待由所述密码算法的一或多个第二阶段使用的密钥；第三组组件，其经配置以将所述密码算法的所述

一或多个第二阶段应用于所述经排列中间数据以产生第二中间数据，所述密码算法的所述一或多个第二阶段使用所述经排列密钥；和第四组组件，其经配置以根据所述预定排列的逆排列而排列所述第二中间数据以产生输出。

[0017] 此电路的实施方案可包含以下特征中的一或多者。第五组组件，其经配置以将所述密码算法的所述一或多个第一阶段应用于待加密的数据以产生所述第一中间数据。第六组组件，其经配置以从一组排列选择排列，其中根据所述预定排列而排列所述第一中间数据的所述次序以产生经排列中间数据包括使用所述所选排列来排列所述第一中间数据的所述次序。所述第六组组件进一步经配置以产生随机数种子值，和基于所述随机数种子值而从所述组排列选择所述排列。所述第六组组件进一步经配置以基于预定模式而从所述组排列选择所述排列。所述第四组组件经配置以基于所述所选排列而从一组逆排列选择所述逆排列。所述密码算法为高级加密标准(AES)算法，且其中所述密码算法的所述一或多个第一阶段包括所述AES算法的第一轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的第二轮；或所述密码算法的所述一或多个第一阶段包括所述AES算法的倒数第二轮，且所述密码算法的所述一或多个第二阶段包括所述AES算法的最后一轮。

## 附图说明

[0018] 图1说明可用以进行对密码算法的功率分析攻击的实例过程。

[0019] 图2为提供对可用以减小对密码算法的功率分析攻击的成功可能性的对策的比较的说明。

[0020] 图3为提供常规AES密码算法的轮与根据本文所揭示的技术的经修改AES密码算法之间的比较的说明。

[0021] 图4说明常规AES-192实施方案的轮与利用本文所揭示的技术的经修改AES-192实施方案之间的比较。

[0022] 图5A为可用以实施常规AES-128算法的电路的功能图。

[0023] 图5B为可用以实施经修改AES-128算法的使用算法变换技术以将随机化引入到AES-128算法中的电路的功能图。

[0024] 图5C为可用以实施经修改AES-128算法的使用算法随机化技术以将随机化引入到AES-128算法中的电路的功能图。

[0025] 图6为可用以实施本文所揭示的技术的移动装置600的框图。

[0026] 图7为说明图6中展示的存储器的功能模块的图6中说明的移动装置的功能框图。

[0027] 图8为可用以实施本文所揭示的加密技术的用于加密数据的过程的流程图。

## 具体实施方式

[0028] 本文所揭示的技术可用以帮助防止对密码算法的旁通道攻击。举例来说，本文所揭示的技术可帮助防止对密码算法的功率分析和/或EM攻击，且还可提供保护以免受对密码算法的其它类型的旁通道攻击。本文所揭示的技术可用以将随机化引入到密码算法中，其可使对密码算法的旁通道攻击难得多。已使用采用高级加密标准(AES)算法的实例说明本文所揭示的技术的实例。然而，本文所揭示的技术还可应用于其它类型的密码算法。本文中的技术可用于基于硬件、基于软件或其组合的密码算法实施方案。

[0029] 图2为提供对可用以减小对密码算法的功率分析攻击的成功可能性的对策的比较的说明。对策可划分成两种类别：(1)隐藏技术，和(2)掩蔽技术。在隐藏技术中，可应用电路层次设计技术以甚至当向密码算法提供不同输入时，也使实施密码算法的数字电路的功率消耗保持大致相同。在掩蔽技术中，密码算法经设计以当算法对数据进行操作时通过使用随机掩码掩蔽数据来使功率消耗随机化，和在完成计算之后移除掩码。本文所揭示的技术是掩蔽技术的变化形式，其帮助使功率消耗随机化，同时执行密码算法以使攻击者分析通过旁通道攻击采集的数据来破解密码算法变得困难得多。

[0030] 原始密码算法205的流程图说明将输入值a提供到密码函数f且密码函数输出经加密版本的输入值a(在图1中称作f(a))。原始密码算法205表示一般密码算法且不限于AES或任何其它特定的加密技术。原始密码算法205并不采取任何步骤以防止功率分析攻击、EM攻击或其它类型的旁通道攻击。因此，原始密码算法205可容易遭受旁通道攻击，其可显露与密码算法相关联的中间数据、与算法相关联的密钥、和/或攻击者可用以破解密码算法的其它信息。

[0031] 掩蔽技术由掩蔽密码算法210说明。掩蔽密码算法210为原始密码算法205的经修改版本，其包含掩蔽和解掩蔽步骤。掩蔽密码算法210可通过密码算法使功率消耗随机化以尝试阻止对密码算法的功率分析和EM攻击。在掩蔽密码算法210中，将掩蔽操作应用于输入值a以使用掩码值m产生经掩蔽输入值$a_m$。接着将经掩蔽输入值$a_m$提供到经掩蔽版本的密码函数$f_m$。接着用解掩蔽操作解掩蔽来自经掩蔽版本的密码函数$f_m$的输出，以便获得在原始密码算法205中获得的f(a)值。掩蔽密码算法210需要修改原始密码函数以使用经掩蔽值进行工作，以便随机化与密码处理相关联的功率消耗。

[0032] 图2还说明本文所揭示的可用以将随机化引入到密码算法中以使对密码算法的功率分析攻击、EM攻击或其它类型的旁通道攻击困难得多的两个技术。第一个技术为算法变换技术且第二个技术为算法随机化技术。两个技术都可用以将随机化添加到密码算法的一个或多个阶段，而不需要在掩蔽密码算法210中那样修改加密函数。

[0033] 变换算法215应用变换函数P，变换函数P在输入值a由加密函数f操作之前排列输入值a。排列重新排序被提供到加密函数f的输入值的字节。加密函数展现轮层次或阶段层次不变性，此意味着可根据变换函数P排列输入的字节的次序，且将次序输入到加密函数f中，而不会影响加密函数f的输出。归因于变换函数P的应用，将排列加密函数f的输出的字节的次序。然而，逆排列函数$P^{-1}$(其为变换函数P的倒数)重新排序加密函数的经排列输出的字节以匹配原始密码算法205的输出。

[0034] 通过每当执行密码算法时从多个排列功能中的一者作出选择而非将相同排列函数应用到输入值a，随机化算法220与变换算法215相比提供额外保护。随机化算法220经配置以从可排列输入值a的字节的次序的两个或更多个变换函数作出选择。在图2中所说明的实例中，使用随机种子值确定选择将哪一变换函数应用于输入值a。接着使用随机种子值以从多个逆排列函数选择对应于排列函数的逆排列函数。其它技术也可用以选择将哪一变换函数应用于输入值a。举例来说，可使用循环或其它选择方案来取代随机种子值以选择将哪一变换函数应用于输入值a。在一些实施方案中，可实施且可使用一或多个固定选择模式来取代随机种子，以确定将应用哪一变换函数。

[0035] 图3为提供常规AES密码算法的轮与根据本文所揭示的技术的经修改AES密码算法

的比较的说明。AES密码算法展现轮层次不变性，此意味着可使用变换函数排列输入数据的字节的次序，以便将额外随机化添加到AES算法。根据本发明，图3的左列说明常规AES密码算法的一轮的输入和输出，且右列说明经修改AES密码算法的一轮的输入和输出。可使用图2中所说明的变换算法或随机化算法技术来实施经修改AES技术。如果应用变换算法技术，则将预先确定将排列应用于输入值的变换算法，且可任选地将排列应用于密码算法的一或多个轮。如果应用随机化算法技术，则将从各自以不同模式排列输入值的字节的多个变换算法中的一者选择将排列应用于输入值的变换算法，或在一些情况下可不应用排列。另外，可将不同变换算法应用于密码算法的不同轮。

[0036] 在表示常规AES密码算法的左列中，到常规AES算法的输入值包括将向其应用密码算法的16个字节的输入数据。在此实例中，通过4×4矩阵表示所述数据。AES密码算法需要使用Rijndael密钥调度表从主要密码密钥导出的每一轮的单独密钥，Rijndael密钥调度表为可用以将短密钥扩展成数个单独轮密钥的技术。因此，可从用于AES会话的主要密码密钥产生轮的适当的密钥，或可能已产生密钥且可从存储器存取密钥。

[0037] 在表示使用本文所揭示的技术的经修改AES密码算法的右列中，根据变换函数而排列输入值和与轮相关联的子密钥两者。变换函数排列输入数据内的字节，且还在执行AES加密函数的轮之前对待在图3中所描绘的AES轮中应用的密钥执行等效排列。不必对AES密码算法进行改变以使排列函数与AES密码算法结合使用，这是因为AES密码算法至少在此轮不变。在右列中所说明的于其中已应用变换技术的AES轮的输出的字节的次序将不同于在图3的左列中所说明的常规AES加密轮的输出的字节的次序。然而，在执行AES密码算法的轮之前，可使用应用于输入数据的排列的逆排列来重新排序于其中已应用变换技术的AES轮的输出的字节的次序。在将逆排列应用于于其中已应用变换技术的输出数据之后，于其中已应用变换技术的输出数据将匹配在图3的左列中所说明的常规AES轮的轮的输出。在所述轮之前排列输入数据的字节会将随机化引入到所述轮，此可使攻击者使用功率分析或EM攻击以破解密码算法变得更困难。

[0038] 图4说明常规AES-192实施方案的轮与利用本文所揭示的技术的经修改AES-192实施方案之间的比较。在图4中说明的实例中，已修改第9和第10轮的部分以保护第10AES轮。然而，本文中所说明的技术可用以保护AES算法的任何轮。另外，本文中所利用的变换技术可应用于其它版本的AES算法，例如AES-192和AES-256，和/或还应用于其它加密技术。AES-128算法使用128位的密钥长度，AES-192算法使用192位的密钥长度，且AES-256算法使用256位的密钥长度。当图4中所说明的实例将本文所揭示的技术应用于AES-192算法时，本文中所描述的技术还可应用于使用具有不同大小的位长度的密钥和/或具有算法的其它变化形式的其它AES算法。

[0039] 针对常规AES-192实施方案和经修改AES-192实施方案两者，来自轮8的输出为A且轮9的密钥输入为K9。在常规AES-192实施方案中，来自轮9的输出为值B且轮10的密钥输入为密钥K10，且来自轮10的输出为值C。在经修改AES-192实施方案中，以与在常规AES-192实施方案中相同的方式执行算法的头八轮。但使用变换函数排列轮9输出且经排列输出为P(B)。还使用与应用于轮9的输出的相同排列函数来排列轮10的密钥K10。使用经排列数据输入矩阵P(B)和经排列密钥P(K10)执行轮10。轮10的输出为$P^{-1}(C)$。接着使用应用于轮9的输出的排列函数的逆排列来逆排列此输出。将逆排列应用于轮10的输出的结果产生密文C，密

文C为常规AES-192实施方案的轮10产生的相同密文输出。

[0040] 实例硬件

[0041] 图5A、5B和5C为说明可用以实施本文所揭示的技术的电路的功能框图。图5A为可用以实施常规AES-128算法的电路的功能图。图5B为可用以实施经修改AES-128算法的使用算法变换技术以将随机化引入到AES-128算法中的电路的功能图。图5C为可用以实施经修改AES-128算法的使用算法随机化技术以将随机化引入到AES-128算法中的电路的功能图。图5B和5C中说明的电路可用以实施图8中说明的过程。尽管图5B和5C中所说明的实例实施例是针对经修改版本的AES-128算法，但是可对实施其它版本的AES密码算法和/或其它密码算法的电路作出类似修改。

[0042] 图5A说明可用以实施常规AES-128算法的轮的电路。所述电路经配置以接收待加密的纯文本消息和可从其中导出与每一轮相关联的轮密钥的密码密钥。所述电路包含表示包含于AES密码算法的每一轮中的SubBytes、ShiftRows和MixColumns步骤的功能块。AES-128算法包含10轮，且在循环回到表示AES-128算法的SubBytes、ShiftRows和MixColumns步骤的功能块之前，在完成当前轮之后即刻将选择下一轮的适当密钥。

[0043] 图5B为可用以实施经修改AES-128算法的使用算法变换技术以将随机化引入到AES-128算法中的电路的功能图。如图5A中所说明的实例，电路经配置以接收待加密的纯文本消息和可从其中导出与每一轮相关联的轮密钥的密码密钥。然而，图5B中所说明的实例电路包含支持算法变换技术的额外组件，算法变换技术可用以排列由AES轮的步骤使用的输入数据的次序。在图5B中说明的实例中，电路包含未包含在实施图5A中所说明的常规AES到128轮的电路中的变换函数块505和多路复用器510。在图5B中所说明的电路中，在MixColumns步骤之前应用变换函数以排列数据的字节的次序。然而，在其它实施方案中，可在AES轮的SubBytes步骤之前或在ShiftRows步骤之前应用变换函数。另外，当不同密码算法由电路实施时，变换函数块505和多路复用器510的置放可改变。将来自ShiftRows步骤功能块的输出馈送到变换函数块505中，变换函数块505根据由变换函数实施的预定排列而排列来自ShiftRows步骤功能块的输出。变换函数块505应用改变由变换函数块505接收的输入数据的字节的次序的排列。接着将经排列数据输出到多路复用器510。多路复用器510可接着在来自ShiftRows步骤功能块的原始输出与由变换函数块505输出的经排列数据之间作出选择。可将选择信号提供到多路复用器510以致使多路复用器510选择来自ShiftRows步骤功能块的原始输出或由变换函数块505输出的经排列数据。因此，电路可经配置以启用或停用在每一轮处的变换函数的使用，从而使功率分析或EM攻击随变换函数而更困难，因为攻击者将不知晓变换函数是否应用于特定轮，或不知晓在特定轮中应用的变换函数为何模式。

[0044] 所述电路还包含逆变换功能块515和多路复用器520。逆变换功能块515接收MixColumns步骤功能块的输出且将逆排列应用于MixColumns步骤功能块的输出。逆变换函数应用逆排列，其将由逆变换功能块515接收的输入的字节重新排序为在由变换函数块505应用排列之前的字节的次序。因此，来自图5B中所说明的电路的特定轮的输出将为与将从图5A中所说明的常规AES-128算法实施方案的对应轮获得的相同的输出值。在轮期间引入随机化可使旁通道攻击更困难，同时不需要对密码算法作出任何改变。

[0045] 图5C为可用以实施经修改AES-128算法的使用算法随机化技术以将随机化引入到

AES-128算法中的电路的功能图。如图5A和5B中所说明的实例，所述电路经配置以接收待加密的纯文本消息和可从其中导出与每一轮相关联的轮密钥的密码密钥。图5C中所说明的电路提供算法随机化的实例。所述电路包含经配置以接收ShiftRows步骤功能块的输出的多个变换函数块555。变换函数块555中的每一者将不同排列应用于由变换函数块接收的输入数据的字节的次序。接着将经排列数据输出到多路复用器560。多路复用器560可接着在来自ShiftRows步骤功能块的原始输出与由变换函数块555中的一者输出的经排列数据之间进行选择。在一些实施方案中，可产生随机种子值575且将其作为确定多路复用器560选择哪一输入的选择值而提供到多路复用器560。其它技术也可用以确定选择值。举例来说，在一些实施方案中，电路可经配置以从确定多路复用器560选择哪一输入的一或多个预定模式作出选择。

[0046] 图5C中所说明的电路还包含多个逆变换函数块565和多路复用器570。逆变换函数块565接收MixColumns步骤功能块的输出，且将逆排列应用于MixColumns步骤功能块的输出。逆变换函数块565中的每一者对应于变换函数块555中的一者，且实施对应变换函数块555的逆排列。逆变换函数应用逆排列，其将由逆变换功能块565接收的输入的字节重新排序为在由变换函数块555应用排列之前的字节的次序。因此，来自图5C中所说明的电路的特定轮的输出将为与将从图5A中所说明的常规AES-128算法实施方案的对应轮获得的相同的输出值。在轮期间引入随机化可使成功的旁通道攻击更困难，同时不需要对密码算法作出任何改变。另外，添加多个可能的排列会提供额外保护，这是因为潜在攻击者将并不知晓在那轮应用于数据的哪一排列(如果有)。

[0047] 图6为可用以实施本文所揭示的技术的移动装置600的框图。移动装置600可用以至少部分地实施图8中所说明的过程。尽管图6中所说明的实例装置为移动装置，但图8中所说明的过程也可实施于其它类型的计算装置中，例如服务器、桌上型计算机系统或包含可执行处理器可读、处理器可执行软件代码的处理器的其它装置。

[0048] 移动装置600包括计算机系统，计算机系统包含通过总线601彼此连接的通用处理器610、数字信号处理器(DSP)620、无线接口625、GNSS接口665和非暂时性存储器660。移动装置600的其它实施方案可包含图6的实例实施方案中未所说明的额外元件，且/或可不包含图6中所说明的实例实施例中所说明的所有元件。举例来说，移动装置600的一些实施方案可不包含GNSS接口665。

[0049] 无线接口625可包含无线接收器、发射器、收发器和/或使得移动装置600能够使用WWAN、WLAN和/或其它无线通信协议发送和/或接收数据的其它元件。无线接口625可包括能够使用多个无线通信标准发射和接收无线信号的一或多个多模式调制解调器。无线接口625通过线632连接到天线634以用于将通信发送到经配置以使用无线通信协议通信的装置，和从所述装置接收通信。尽管图6中所说明的移动装置600包括单个无线接口625和单个天线634，但移动装置600的其它实施方案可包含多个无线接口625和/或多个天线634。

[0050] 全球导航卫星系统(GNSS)接口665可包含无线接收器和/或使得移动装置600能够从与一或多个GNSS系统相关联的发射器接收信号的其它元件。GNSS接口665通过线672连接到天线674以用于从GNSS发射器接收信号。移动装置600可经配置以使用从与卫星相关联的卫星和与GNSS系统相关联的其它发射器接收的信号，以确定移动装置600的位置。移动装置600还可经配置以使用从GNSS卫星和与GNSS系统相关联的其它发射器接收的信号，结合从

地面无线发射器接收的信号以确定移动装置600的位置。

[0051] DSP 620可经配置以处理从无线接口625和/或GNSS接收器665接收的信号，且可经配置以针对实施为存储在存储器660中的处理器可读、处理器可执行软件代码的一或多个模块或与其结合来处理信号，和/或可经配置以与处理器610结合来处理信号。

[0052] 处理器610可为智能装置，例如个人计算机中央处理单元(CPU)(例如，由Intel®公司或AMD®制造的CPU)、微控制器、专用集成电路(ASIC)等。存储器660为可包含随机存取存储器(RAM)、只读存储器(ROM)或其组合的非暂时性存储装置。存储器660可存储含有用于控制处理器610以执行本文中所描述的功能的指令的处理器可读、处理器可执行软件代码(尽管描述可能说明软件执行功能)。可通过经由网络连接下载、从磁盘上传等将软件载入于存储器660上。另外，软件可并非可直接执行的(例如，要求在执行之前进行编译)。

[0053] 存储器660中的软件经配置以使得处理器610能够执行各种动作，包含实施将数据发送到无线发射器、无线基站、其它移动装置和/或经配置用于无线通信的其它装置和/或从这些装置接收数据。

[0054] 图7为说明图6中展示的存储器660的功能模块的图6中说明的移动装置600的功能框图。举例来说，移动装置600可包含加密模块762和数据存取模块768。移动装置600还可包含向移动装置600提供其它功能性的一或多个额外功能模块。图6和7中所说明的移动装置600可用以实施图8中所说明的过程。

[0055] 加密模块762可经配置以根据本文所揭示的算法变换和/或算法随机化技术而对配置数据进行加密。加密模块762可经配置以实施可用以对数据进行加密的一或多个密码算法。加密模块762可经配置以针对移动装置600上的一或多个应用对数据进行加密。举例来说，加密模块762可经配置以对从在移动装置600上操作的应用接收的数据进行加密，以防止对数据的未经授权存取。加密模块762可经配置以通过向数据存取模块768提供经加密数据来将经加密数据存储在存储器660中。加密模块762还可经配置以对从在移动装置600上操作的应用接收的数据进行解密。举例来说，在移动装置上运行的电子邮件应用可下载具有经加密附件的电子邮件，且如果对附件进行解密所需的密钥对加密模块762可用，则电子邮件应用可经配置以对经加密附件进行解密。

[0056] 加密模块762可经配置以存取可由通过加密模块762实施的密码算法的一或多个阶段使用的一或多个密钥。加密模块762可经配置以将密钥存储于存储器260的防护区或移动装置600的存取受限的其它存储器中。加密模块762可经配置以经由数据存取模块768存取一或多个密钥。加密模块762可经配置以使用密钥以对数据进行加密和/或解密。

[0057] 数据存取模块768可经配置以将数据存储于存储器660和/或与移动装置600相关联的其它数据存储装置中。数据存取模块768还可经配置以存取存储器660和/或与移动装置600相关联的其它数据存储装置中的数据。数据存取模块768可经配置以从移动装置600的其它模块和/或组件接收请求，且将数据存储于存储器660和/或与移动装置600相关联的其它数据存储装置中，和/或存取其中的数据。

[0058] 实例实施方案

[0059] 图8为可用以实施本文所揭示的加密技术的用于加密数据的过程的流程图。图8中所说明的过程可以硬件、软件或其组合予以实施。举例来说，图8中所说明的过程可由图6和7中所说明的移动装置600实施。图8中所说明的过程还可实施于电路中，例如图5中所说明

的实例电路。

[0060] 可将密码算法的一或多个第一阶段应用于待加密的数据以产生第一中间数据(阶段805)。待应用的密码算法的一或多个第一阶段可取决于算法的哪一阶段提供了保护和多少阶段包含于密码算法的特定实施方案中。举例来说,在密码算法为AES密码算法的一些实施方案中,所执行的轮的数目取决于由所述特定实施方案使用的密钥长度。AES-128算法使用128位的密钥长度,AES-192算法使用192位的密钥长度,且AES-256算法使用256位的密钥长度。密钥大小影响将执行的轮的数目。举例来说,AES-128实施方案通常包含10轮,AES-192实施方案通常包含12轮,且AES-256实施方案通常包含14轮。

[0061] 对AES算法的一个共同攻击点在第一轮与第二轮之间。对AES算法的另一个共同攻击点在倒数第二轮与最后一轮之间。举例来说,对AES-128算法的一个共同攻击点在第9轮与第10轮之间,对AES-192算法的一个共同攻击点在第11轮与第12轮之间,且对AES-256算法的一个共同攻击点在第13轮与第14轮之间。因此,密码算法的一或多个第一阶段可为AES算法中的一者的第一轮。密码算法的一或多个第一阶段还可指AES算法的倒数第二轮,例如AES-128算法的第9轮、AES-192算法的第10轮和AES-256算法的第13轮。倒数第二轮的数目可针对其它密码算法而改变。

[0062] 攻击者可使用功率分析攻击(例如上文描述的功率分析攻击),以观察在一段时间内其中已实施密码算法的装置的电活动以产生功率轨迹。功率轨迹可用以提取由算法使用的密码密钥。

[0063] 可根据预定排列而排列第一中间数据的次序以产生经排列中间数据(阶段810)。可根据预定排列模式而排列第一中间数据的字节的次序以产生经排列中间数据。在一些实施方案中,可根据类似于图2中所说明的算法变换技术214的算法变换技术的算法变换技术而执行预定排列。在算法变换技术中,可在于其中实施密码算法的软件和/或硬件中实施变换函数。变换函数可根据预定模式而重新排序输入数据的字节,一旦已将密码算法的下一阶段或接下来的多个阶段应用于输入数据,则可使用逆排列函数逆转预定模式。图3说明将此类变换函数应用于AES密码算法的轮的输入数据的实例。16个字节的输入数据表示为4×4数据矩阵。变换函数排列输入数据的字节的次序以使得输入数据的字节不再以当从先前AES轮输出时所处的相同次序定位。在其它实施方案中,可使用类似于图2中所说明的随机化算法220的算法随机化技术的算法随机化技术。在算法随机化技术中,用以排列输入数据的变换函数并非静态且可选自多个预定排列函数。举例来说,算法随机化技术的特定实施方案可包含各自以不同模式排列输入数据的一组五个变换函数。算法随机化技术还可实施用于选择将应用于输入数据的五个预定变换中的一者的装置。随机地选择变换算法中的一者以排列输入数据可使尝试揭露正使用的密钥的对密码算法的功率分析和其它类型的攻击变得困难得多。在一些实施方案中,可产生随机种子值且将其馈送到多路复用器中,所述多路复用器选择将应用于输入数据的变换函数。对于如上文所论述的算法变换和算法随机化技术两者,如果可能,则应使所使用的排列模式保密。其它技术还可用以选择将应用哪一变换函数。举例来说,可使用轮循或其它选择方案来取代随机种子值,以选择将应用哪一变换函数。在一些实施方案中,可实施且可使用一或多个固定选择模式来取代随机种子,以选择将应用哪一变换函数。

[0064] 可根据预定排列而排列待由密码算法的一或多个第二阶段使用的密钥(阶段

815)。还可根据已应用于输入值的相同的变换算法变换而排列由待在第一中间数据上操作的密码算法使用的密钥。图3中所说明的实例提供使用与输入数据相同的变换算法来排列密钥的实例。密钥可由密码算法的多个阶段使用,或可特定针对密码算法的一个阶段。举例来说,AES算法需要使用Rijndael密钥调度表从主要密码密钥导出的每一轮的单独密钥,Rijndael密钥调度表为可用以将短密钥扩展成数个单独轮密钥的技术。

[0065] 可将密码算法的一或多个第二阶段应用于经排列中间数据以产生第二中间数据(阶段820)。密码算法的一或多个第二阶段可使用在阶段815中产生的经排列密钥。图3中所说明的实例提供将AES轮的步骤应用于经排列中间数据的实例,经排列中间数据在图3的实例中为由AES算法的先前轮输出的4×4矩阵的输入值。来自阶段815的经排列密钥也用于AES轮中。在本文所揭示的技术应用于其它密码算法的情况下,由密码算法的一或多个第二阶段使用的密钥的输入值和/或类型可不同于用于提供于图3中的AES实例中的输入值和/或类型。

[0066] 可根据预定排列的逆排列而排列第二中间数据以产生输出(阶段825)。可使用在阶段810和820中应用的排列的逆排列排列第二中间数据,以产生与未经修改的密码算法的一或多个第二阶段的输出将产生的输出相同的输出。举例来说,返回参看图3的实例,与经应用以排列输入日期的变换函数和与那一轮相关联的子密钥相关联的逆排列被应用于经排列中间数据以重新排序经排列中间数据的字节以使得字节处于在应用常规AES密码算法而非本文所揭示的经修改密码技术的情况下字节将处于的相同次序中。因此,本文所揭示的技术并不需要修改由密码算法在阶段或轮中的每一者中执行的操作以与这些技术协作。可在可由功率分析攻击、EM攻击和/或其它类型的旁通道攻击定为目标的密码算法的一个或多个阶段或轮处应用所述技术。

[0067] 来自阶段825的输出可用作到密码算法的一或多个后续阶段的输入。举例来说,在密码算法为AES算法的情况下且在密码算法的一或多个第二阶段对应于AES算法中的一者的轮2的情况下,来自轮2的输出将在密文由算法输出之前由若干额外轮处理。在密码算法为AES算法的情况下且在密码算法的一或多个第二阶段对应于AES算法中的一者的最后一轮的情况下,来自最后一轮的输出将在密文由算法输出之前由若干额外轮处理。

[0068] 取决于应用,可通过各种装置来实施本文中所描述的方法。举例来说,这些方法可在硬件、固件、软件或其任何组合中实施。对于硬件实施方案,处理单元可实施于一或多个专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理装置(DSPD)、可编程逻辑装置(PLD)、现场可编程门阵列(FPGA)、处理器、控制器、微控制器、微处理器、电子装置、经设计以执行本文中所描述功能的其它电子单元,或其组合内。

[0069] 对于固件和/或软件实施方案,可用执行本文所描述的功能的模块(例如,程序、功能等等)来实施方法。在实施本文所描述的方法时,可使用有形地体现指令的任何机器可读媒体。举例来说,软件代码可存储在存储器中,并且由处理器单元来执行。存储器可实施在处理器单元内或处理器单元外部。如本文中所使用的术语“存储器”是指任何类型的长期、短期、易失性、非易失性或其它存储器,且并不限于任何特定类型的存储器或特定数目的存储器或特定类型的媒体。有形媒体包含机器可读媒体的一或多个物理物品,例如随机存取存储器、磁性存储装置、光学存储媒体等等。

[0070] 如果以固件和/或软件实施,那么可将所述功能作为一或多个指令或代码存储在

计算机可读媒体上。实例包含用数据结构编码的计算机可读媒体和用计算机程序编码的计算机可读媒体。计算机可读媒体包含物理计算机存储媒体。存储媒体可为可由计算机存取的任何可用的媒体。作为实例而非限制，此种计算机可读媒体可包括RAM、ROM、EEPROM、CD-ROM或其它光盘存储器，磁盘存储器或其它磁性存储装置，或任何其它可用于存储呈指令或数据结构形式的所要程序代码且可由计算机存取的媒体；如本文中所使用，磁盘和光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能光盘(DVD)，软性磁盘和蓝光光盘，其中磁盘通常以磁性方式再现数据，而光盘用激光以光学方式再现数据。以上各者的组合也应该包含在计算机可读媒体的范围内。此类媒体也提供可为机器可读的非暂时性媒体的实例，且其中计算机为可从此类非暂时性媒体进行读取的机器的实例。

[0071] 在不脱离本发明或权利要求的精神或范围的情况下，本文中所论述的一般原理可应用于其它实施方案。

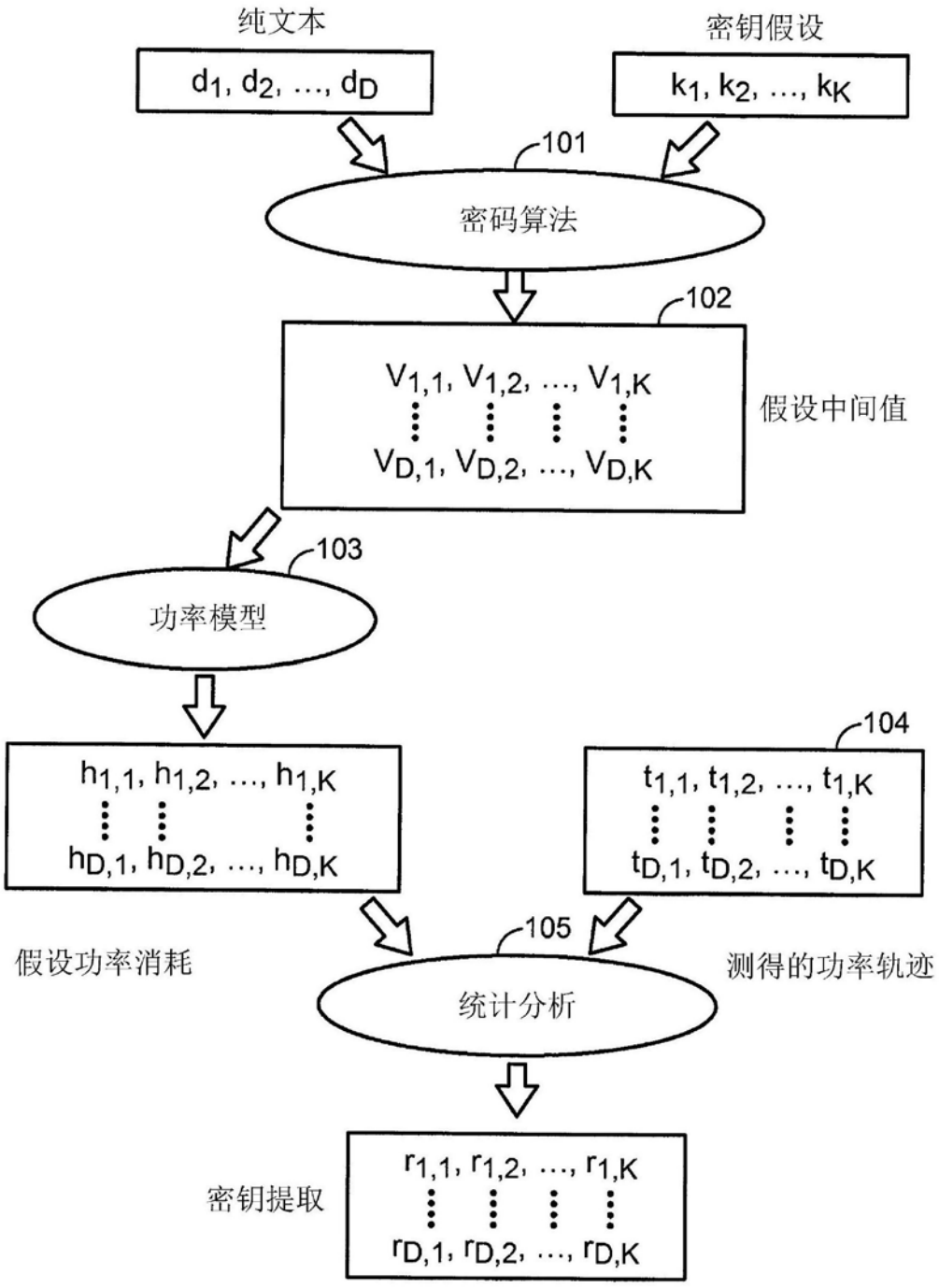

纯文本
密钥假设
$d_1, d_2, \ldots, d_D$
$k_1, k_2, \ldots, k_K$
101
密码算法
102
$V_{1,1}, V_{1,2}, \ldots, V_{1,K}$
$V_{D,1}, V_{D,2}, \ldots, V_{D,K}$
假设中间值
103
功率模型
$h_{1,1}, h_{1,2}, \ldots, h_{1,K}$
$h_{D,1}, h_{D,2}, \ldots, h_{D,K}$
104
$t_{1,1}, t_{1,2}, \ldots, t_{1,K}$
$t_{D,1}, t_{D,2}, \ldots, t_{D,K}$
假设功率消耗
105
测得的功率轨迹
统计分析
密钥提取
$r_{1,1}, r_{1,2}, \ldots, r_{1,K}$
$r_{D,1}, r_{D,2}, \ldots, r_{D,K}$

图1

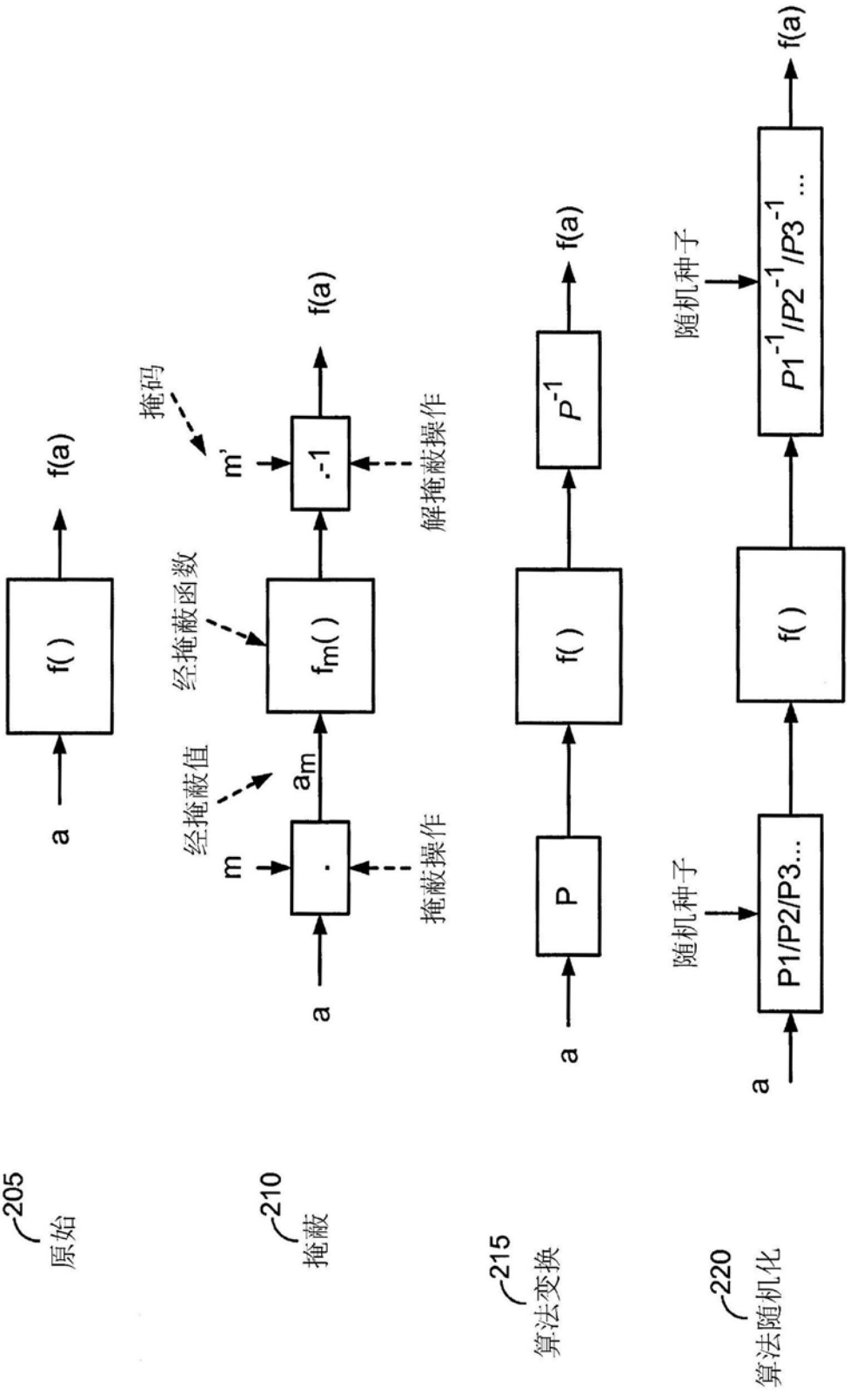

205
原始
a
f( )
f(a)
210
掩蔽
a
m
掩蔽操作
经掩蔽值
经掩蔽函数
$f_m( )$
.-1
掩码
m'
解掩蔽操作
f(a)
215
算法变换
a
P
f( )
$P^{-1}$
f(a)
220
算法随机化
a
随机种子
P1/P2/P3...
f( )
随机种子
$P1^{-1}/P2^{-1}/P3^{-1}$ ...
f(a)

图2

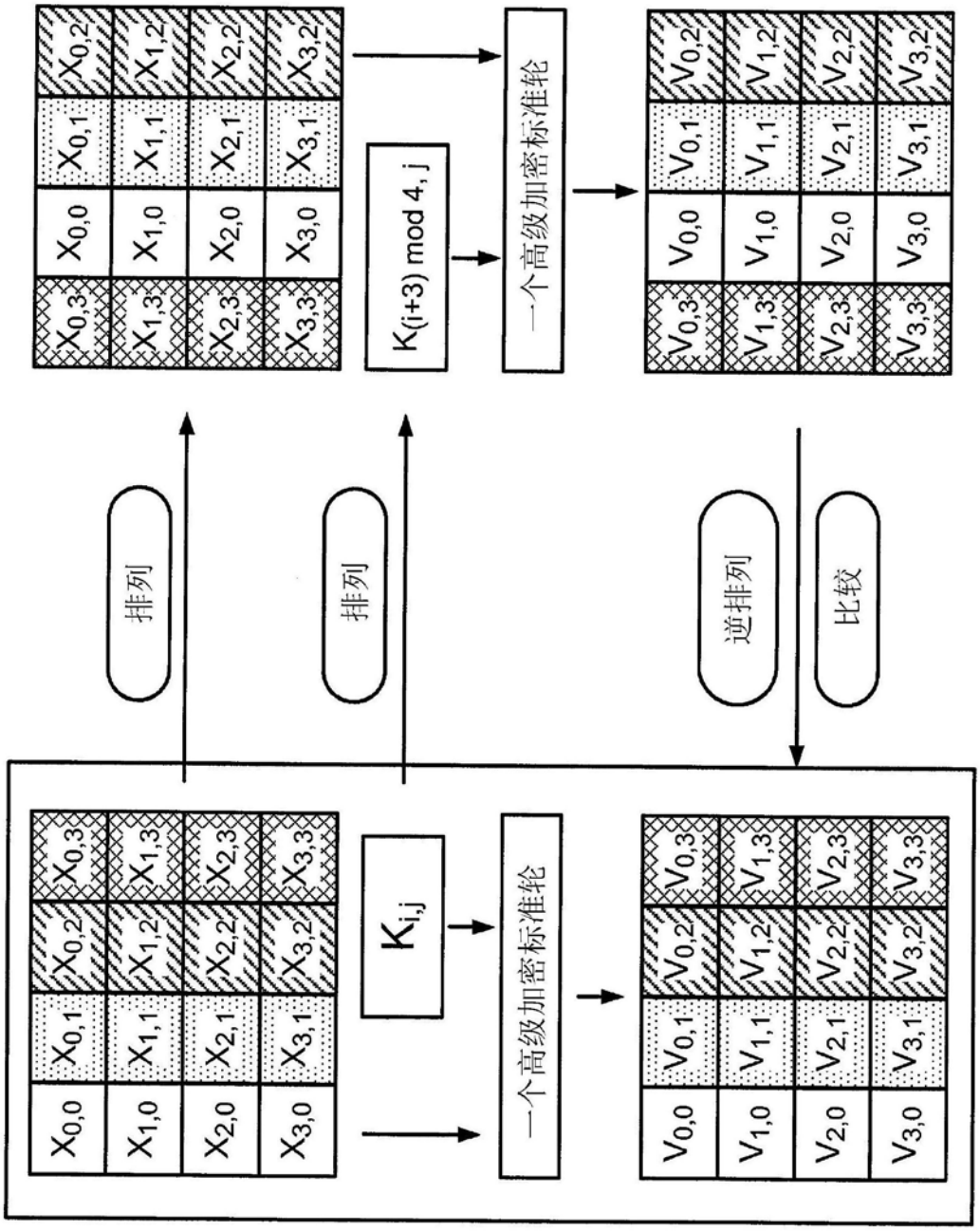

$X_{0,2}$ $X_{1,2}$ $X_{2,2}$ $X_{3,2}$
$X_{0,1}$ $X_{1,1}$ $X_{2,1}$ $X_{3,1}$
$X_{0,0}$ $X_{1,0}$ $X_{2,0}$ $X_{3,0}$
$X_{0,3}$ $X_{1,3}$ $X_{2,3}$ $X_{3,3}$
$K_{(i+3) \bmod 4, j}$
一个高级加密标准轮
$V_{0,2}$ $V_{1,2}$ $V_{2,2}$ $V_{3,2}$
$V_{0,1}$ $V_{1,1}$ $V_{2,1}$ $V_{3,1}$
$V_{0,0}$ $V_{1,0}$ $V_{2,0}$ $V_{3,0}$
$V_{0,3}$ $V_{1,3}$ $V_{2,3}$ $V_{3,3}$
排列
排列
逆排列
比较
$X_{0,3}$ $X_{1,3}$ $X_{2,3}$ $X_{3,3}$
$X_{0,2}$ $X_{1,2}$ $X_{2,2}$ $X_{3,2}$
$X_{0,1}$ $X_{1,1}$ $X_{2,1}$ $X_{3,1}$
$X_{0,0}$ $X_{1,0}$ $X_{2,0}$ $X_{3,0}$
$K_{i,j}$
一个高级加密标准轮
$V_{0,3}$ $V_{1,3}$ $V_{2,3}$ $V_{3,3}$
$V_{0,2}$ $V_{1,2}$ $V_{2,2}$ $V_{3,2}$
$V_{0,1}$ $V_{1,1}$ $V_{2,1}$ $V_{3,1}$
$V_{0,0}$ $V_{1,0}$ $V_{2,0}$ $V_{3,0}$

图3

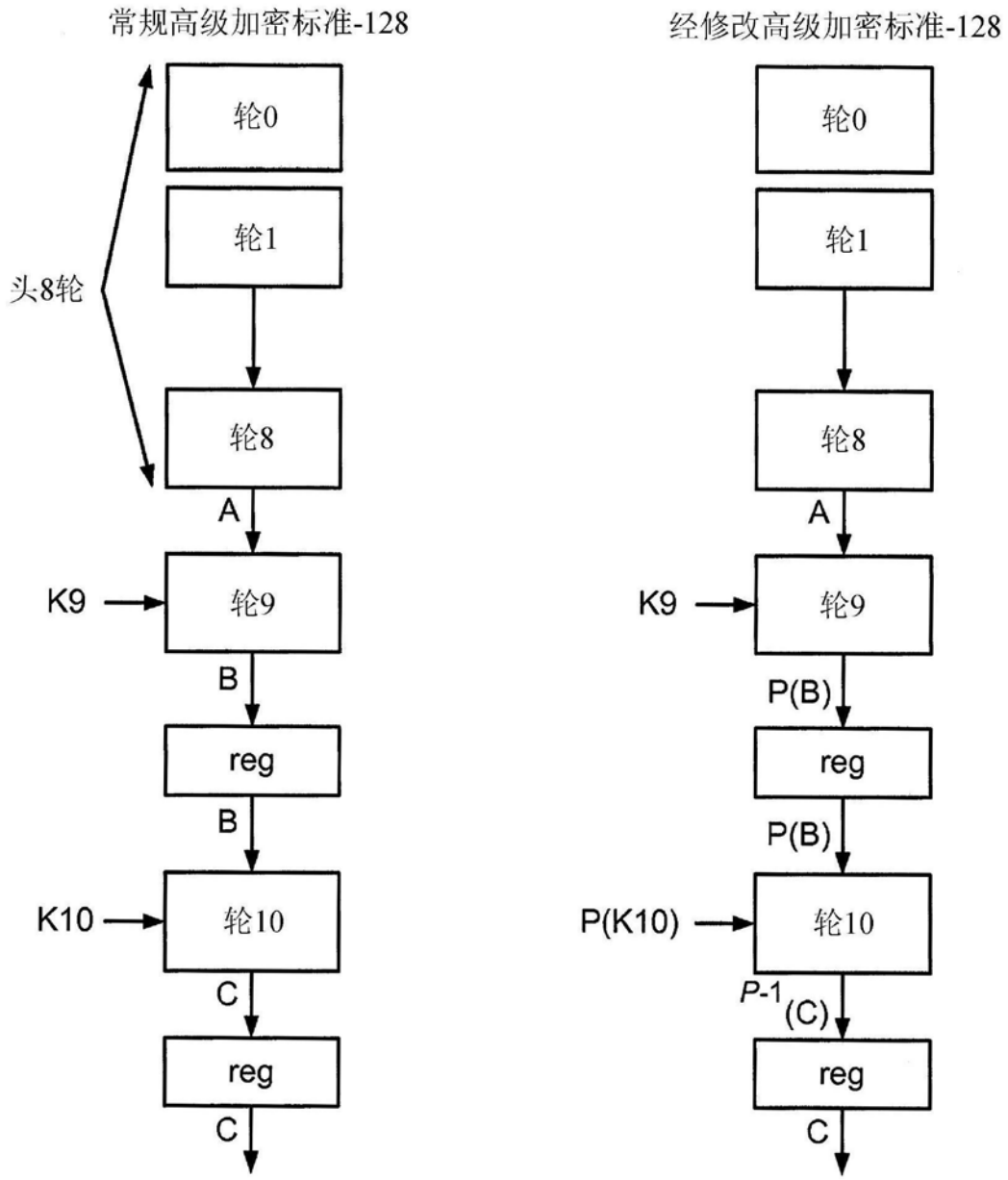

常规高级加密标准-128
轮0
轮1
头8轮
轮8
A
K9
轮9
B
reg
B
K10
轮10
C
reg
C
经修改高级加密标准-128
轮0
轮1
轮8
A
K9
轮9
P(B)
reg
P(B)
P(K10)
轮10
P-1(C)
reg
C

图4

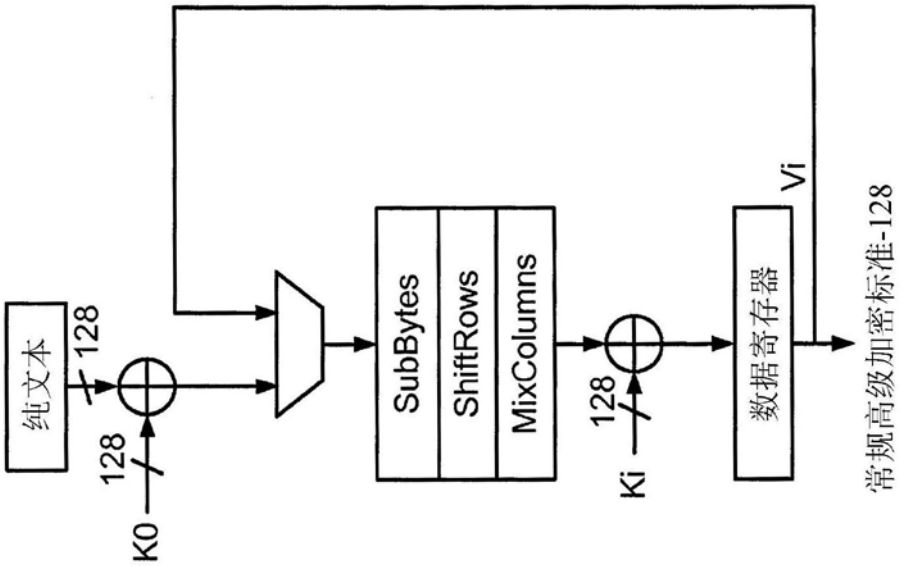

纯文本
128
128
K0
SubBytes
ShiftRows
MixColumns
128
Ki
数据寄存器
Vi
常规高级加密标准-128

图5A

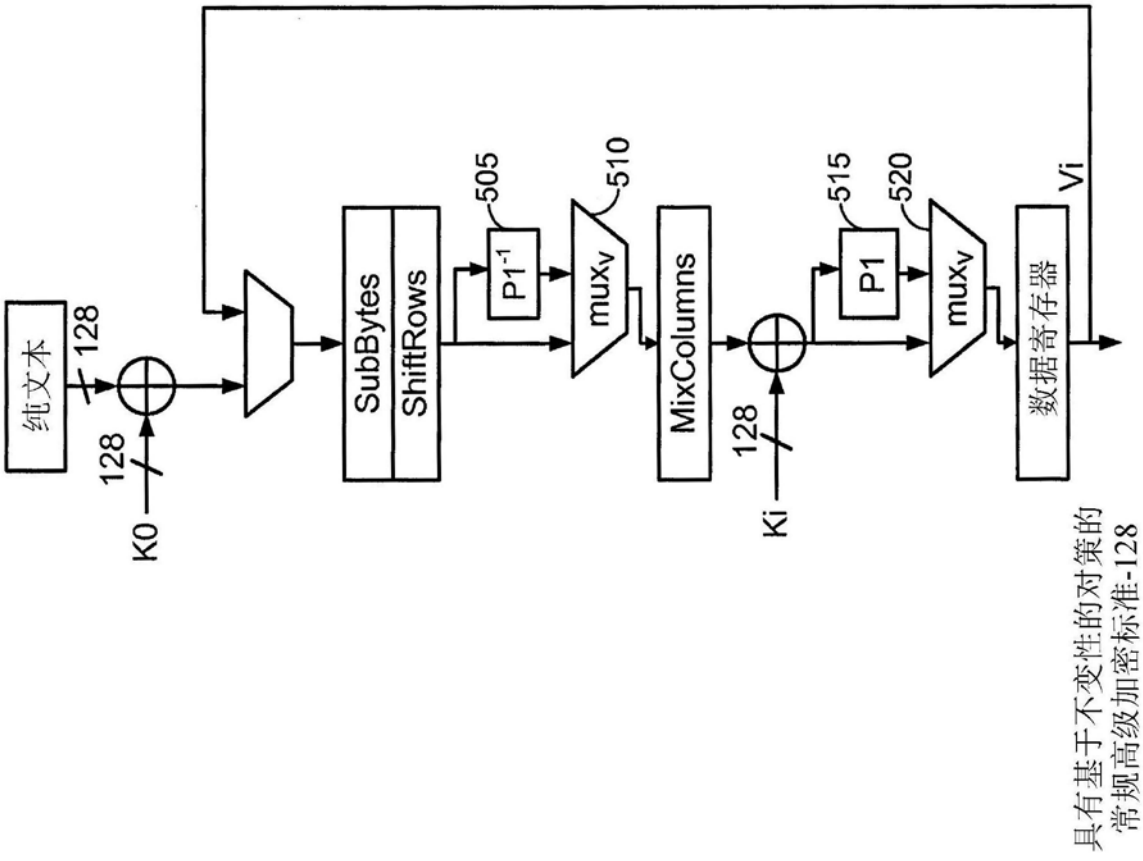

纯文本
128
128
K0
SubBytes
ShiftRows
505
P1-1
510
muxv
MixColumns
128
Ki
515
P1
520
muxv
数据寄存器
Vi
具有基于不变性的对策的
常规高级加密标准-128

图5B

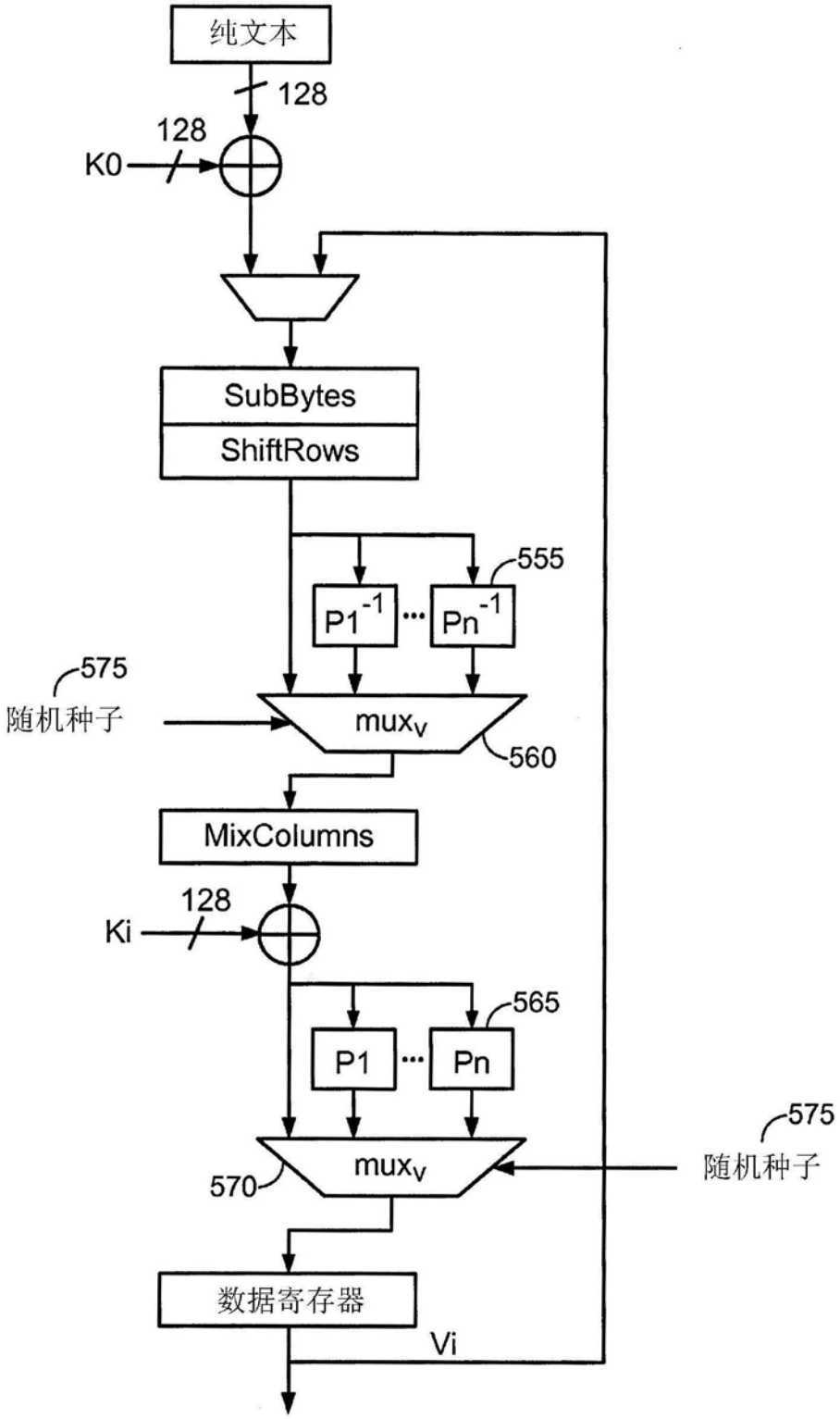

纯文本
128
128
K0
SubBytes
ShiftRows
555
P1-1
Pn-1
575
随机种子
muxV
560
MixColumns
128
Ki
565
P1
Pn
575
随机种子
muxV
570
数据寄存器
Vi

图5C

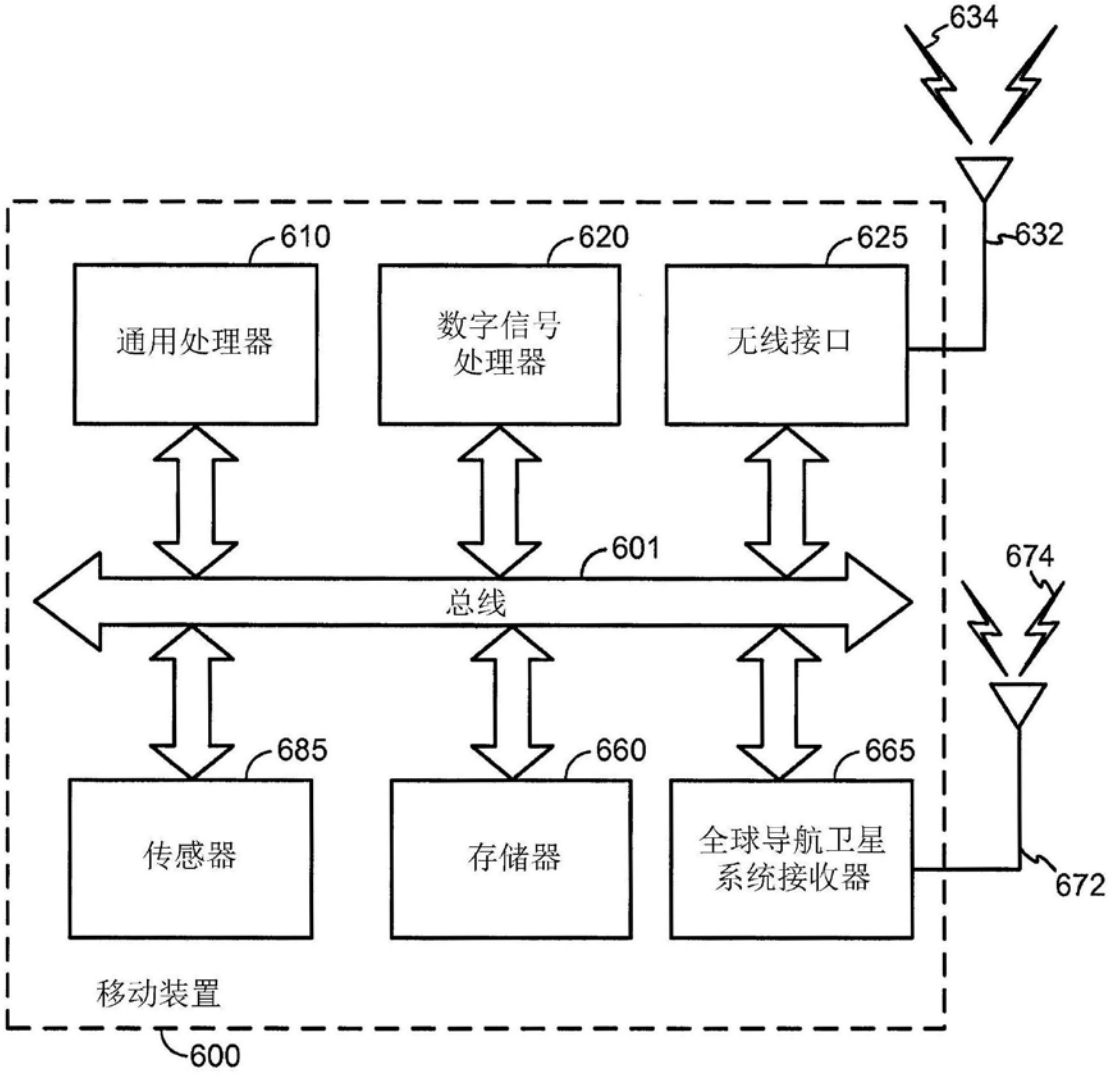

634
632
610
620
625
通用处理器
数字信号
处理器
无线接口
601
总线
674
685
660
665
传感器
存储器
全球导航卫星
系统接收器
672
移动装置
600

图6

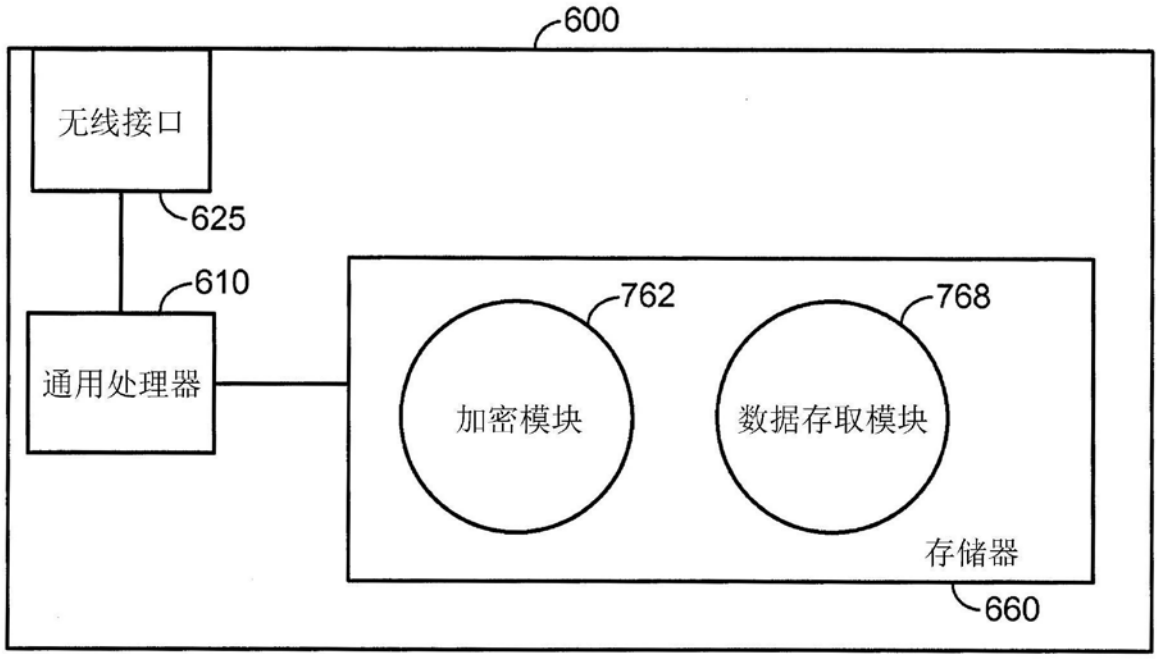
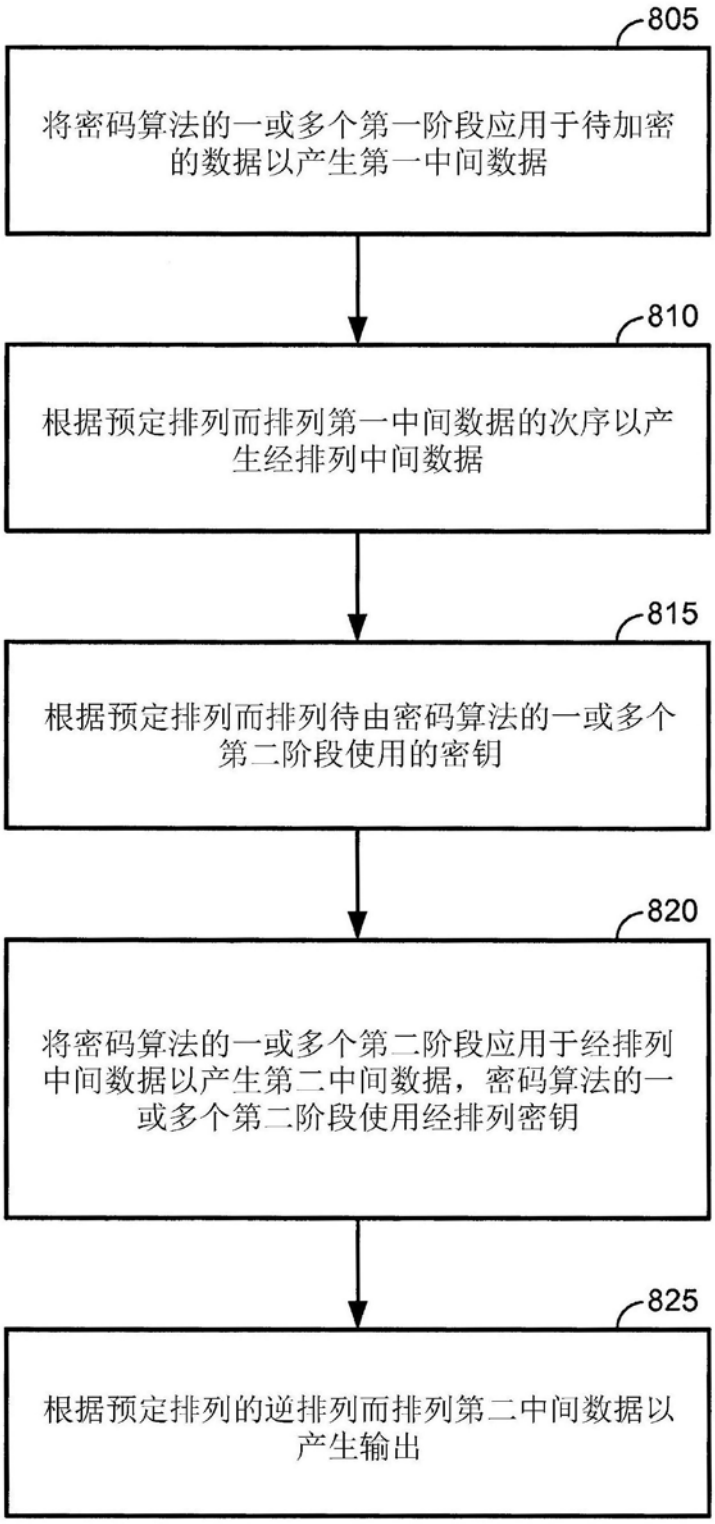



图7


805
将密码算法的一或多个第一阶段应用于待加密的数据以产生第一中间数据
810
根据预定排列而排列第一中间数据的次序以产生经排列中间数据
815
根据预定排列而排列待由密码算法的一或多个第二阶段使用的密钥
820
将密码算法的一或多个第二阶段应用于经排列中间数据以产生第二中间数据，密码算法的一或多个第二阶段使用经排列密钥
825
根据预定排列的逆排列而排列第二中间数据以产生输出

加密过程

图8