(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 103842212 B
(45)授权公告日 2017.05.31

(21)申请号 201280048727.6
(22)申请日 2012.09.12
(65)同一申请的已公布的文献号
申请公布号 CN 103842212 A
(43)申请公布日 2014.06.04
(30)优先权数据
61/533,590 2011.09.12 US
13/610,377 2012.09.11 US
(85)PCT国际申请进入国家阶段日
2014.04.03
(86)PCT国际申请的申请数据
PCT/US2012/054728 2012.09.12
(87)PCT国际申请的公布数据
WO2013/039952 EN 2013.03.21
(73)专利权人 密克罗奇普技术公司
地址 美国亚利桑那州
(72)发明人 维维安·德尔波
麦可·A·史达基
恩里克·阿莱曼
(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 沈锦华
(51)Int.Cl.
B60R 16/00(2006.01)
H04L 9/06(2006.01)
H04W 12/02(2009.01)
H04W 12/06(2009.01)
(56)对比文件
WO 00/18060 A2,2000.03.30,
CN 1752996 A,2006.03.29,
US 6760439 B1,2004.07.06,
CN 101393658 A,2009.03.25,
US 2011/0064093 A1,2011.03.17,
US 2011/0051514 A1,2011.03.03,
US 5303303 A,1994.04.12,
审查员 严晨枫

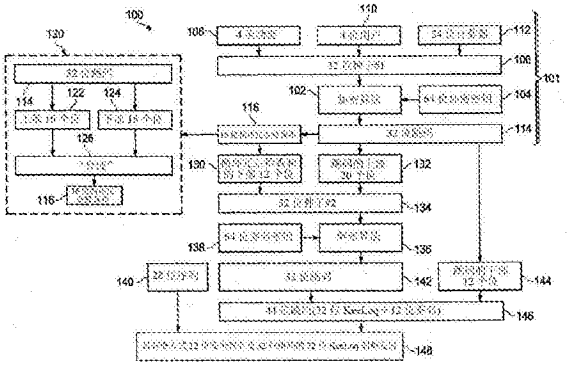
权利要求书2页 说明书6页 附图3页

(54)发明名称

具有增加的安全性的基于跳码的系统

(57)摘要

本发明揭示一种接入系统，其包含用于交换安全数据的发射器及接收器，其中所述系统使用加密及解密算法来交换安全数据包。所述安全数据包可包含未经加密数据包及经加密数据包。所述经加密数据包可包含通过所述加密算法加密的第一数据及通过所述解密算法解密的数据，其中通过所述解密算法解密的所述数据包含安全签名与通过所述加密算法加密的第二数据的组合。



CN 103842212 B

1.一种无线接入系统,其包括:

发射器及接收器,其用于交换安全数据,其中所述系统使用加密及解密算法来交换安全数据包,所述解密算法逆向于所述加密算法,其中所述加密是块密码加密,且其中所述发射器经配置为产生所述安全数据包用于发射,所述安全数据包包括:

未经加密数据包,

经加密数据包,其中所述经加密数据包包括:

通过所述加密算法加密的第一数据的第一部分,

通过所述解密算法解密的第二数据,其中所述解密算法接收所述第一数据的第二部分与安全签名的组合,其中所述安全签名由所述第一数据导出。

2.根据权利要求1所述的无线接入系统,

其中所述安全数据包包括计数器、计时器或伪随机值、功能值或用户定义的位。

3.根据权利要求1所述的无线接入系统,其中所述安全签名是通过CRC算法由所述第一数据导出的。

4.根据权利要求1所述的无线接入系统,其中所述安全签名是通过杂凑算法由所述第一数据导出的。

5.根据权利要求1所述的无线接入系统,

其中所述加密及解密算法使用不同的签名密钥。

6.根据权利要求5所述的无线接入系统,其中用于所述解密算法的签名密钥对每一发射器是唯一的。

7.根据权利要求1所述的无线接入系统,

其中所述未经加密数据包被包含到所述经加密数据包中。

8.根据权利要求1所述的无线接入系统,其中所述发射器是无线发射器。

9.根据权利要求1所述的无线接入系统,还包括:

控制器,其包含计算机程序产品,所述计算机程序产品包括用于实施所述加密及解密算法的一个或多个非暂时性机器可读媒体。

10.一种无线接入方法,其包括:

产生用于发射的安全数据包,所述产生包含

产生未经加密数据包;及

产生经加密数据包,其中所述经加密数据包包括:

通过加密算法加密的第一数据的第一部分,

通过解密算法解密的第二数据,其中所述解密算法接收安全签名与所述第一数据的第二部分的组合,其中所述安全签名由所述第一数据导出;及

通过发射器将所述用于发射的安全数据包发射到接收装置。

11.根据权利要求10所述的无线接入方法,

其中所述安全数据包包括计数器、计时器或伪随机值、功能值或用户定义的位。

12.根据权利要求10的所述无线接入方法,其中通过CRC算法从所述第一数据导出所述安全签名。

13.根据权利要求10的所述无线接入方法,其中通过杂凑算法从所述第一数据导出所述安全签名。

14.根据权利要求10所述的无线接入方法，其中所述加密及解密算法使用不同的签名密钥。

15.根据权利要求14所述的无线接入方法，其中用于所述解密算法的签名密钥对每一发射器是唯一的。

16.根据权利要求10所述的无线接入方法，其中将所述未经加密数据包包含到所述经加密数据包中。

17.根据前述权利要求12-16中任一项所述的无线接入方法，其进一步包括在所述接收装置处解密所述用于发射的安全数据包以获得经解密数据并使用所述经解密数据来控制锁或电机。

18.根据前述权利要求12-16中任一项所述的无线接入方法，其中所述用于发射的安全数据包是无线地执行的。

19.一种使用加密及解密算法来交换安全数据包的发射器，所述解密算法逆向于所述加密算法，其中所述加密是块密码加密，所述发射器经配置为装配安全数据包，所述安全数据包包括：

未经加密数据包，

经加密数据包，其中所述经加密数据包包括：

通过所述加密算法加密的第一数据的第一部分，

通过所述解密算法解密的第二数据，其中所述解密算法接收所述第一数据的第二部分与安全签名的组合，其中所述安全签名由所述第一数据导出。

20.根据权利要求19所述的发射器，其中所述接收器是包括锁定装置的无线接收器。

具有增加的安全性的基于跳码的系统

[0001] 相关申请案交叉参考

[0002] 本申请案主张2011年9月12日申请的标题为“具有增加的安全性的基于跳码的系统(Code Hopping Based System with Increased Security)”的第61/533,590号美国临时申请案的优先权,所述申请案特此以全文引用的方式并入本文中,如同在本文中全面地陈述。

技术领域

[0003] 本发明涉及具有增加的安全性的跳码系统。

背景技术

[0004] 无钥匙进入系统(例如用于车库开门器及无钥匙汽车锁的无钥匙进入系统)通常采用无线电发射器来将指令发送到无线电接收器,所述指令接着致使将门打开或关闭(或锁定及解锁)。此些系统通常采用跳码来防止“重放”攻击,其中窃听者记录发射且在稍后时间处将其重放以将门打开或解锁。

[0005] 广泛使用的跳码系统为可从微芯片(Microchip)技术有限公司购得的KeeLoq。传统KeeLoq采用非线性反馈移位寄存器(NLFSR)且借助64位加密密钥对32位块进行加密。较新KeeLoq系统还使用其它流行加密系统,包含基于XTEA(扩展式微型加密算法)或AES-128(高级加密标准)的那些加密系统。XTEA采用具有128位密钥的64位块密码,而AES-128使用128位块及128位密钥。

[0006] 增加安全性系统的安全性通常需要使用较强加密算法、使用较长加密密钥、多个加密密钥/计算或这些方法的组合。举例来说,在同一系统内使用一个以上64位加密密钥意味着任何强力型攻击方案均需要计算更多的密钥组合才能攻击系统的安全性。

[0007] 所有块密码算法(例如与KeeLoq一起使用的块密码算法)通常对固定块大小(对于传统KeeLoq加密来说为32个位,或对于使用AES-128加密的KeeLoq系统来说为128个位)起作用。因此,举例来说,为了从一个块密码算法(NLFSR)跳转或升级到另一块密码算法(AES-128)需要显著增加所需要的数据位的数目。此可使现有RF(射频)设计复杂化,或许甚至需要系统重新设计,或在替代方案中,接受整体系统性能的降低。

[0008] 换句话说,为了增加基于无线的接入系统的安全性,可使用通常需要发射更多数据位的替代加密算法。然而,使用较大加密块需要发射较多数据位。较多位通常意味着较慢反应时间或数据发射的位速率的增加。此两者需要当前RF设计的重新设计,此可为昂贵且耗费时间的。

发明内容

[0009] 根据一些实施例的无线接入系统包含用于交换安全数据的发射器及接收器,其中所述系统使用加密及解密算法来交换安全数据包。所述安全数据包可包含未经加密数据包及经加密数据包。所述经加密数据包可包含通过所述加密算法加密的第一数据及通过所述

解密算法解密的数据，其中通过所述解密算法解密的所述数据包含安全签名与通过所述加密算法加密的第二数据的组合。

[0010] 根据一些实施例的无线接入方法包含通过产生未经加密数据包及产生经加密数据包来产生经译码发射。所述经加密数据包可包含通过加密算法加密的第一数据及通过解密算法解密的数据，其中通过所述解密算法解密的所述数据包括安全签名与通过所述加密算法加密的第二数据的组合。最后，所述方法可包含将经译码发射发射到接收装置。

[0011] 当结合以下描述及随附图式考虑时，将更佳地了解及理解本发明的这些及其它方面。然而，应理解，尽管指示本发明的各种实施例及其众多特定细节，但以下描述是以图解说明方式而非限制方式给出。可在不背离本发明的精神的情况下在本发明的范围内做出许多替代、修改、添加及/或重新布置，且本发明包含所有此类替代、修改、添加及/或重新布置。

附图说明

[0012] 所属领域的技术人员可通过参考随附图式更佳地理解本发明且明了本发明的众多目标、特征及优点。在不同图式中使用相同参考符号来指示类似或相同物项。

[0013] 图1是图解说明示范性无线进入系统的图式。

[0014] 图2是图解说明示范性经加密码字的图式。

[0015] 图3是图解说明计算码字的示范性方法的图式。

[0016] 图4是图解说明无线接入系统的操作的流程图。

具体实施方式

[0017] 参考在随附图式中图解说明且在以下描述中详述的示范性且因此非限制性实施例更全面地阐释本发明及其各种特征及有利细节。可省略已知编程技术、计算机软件、硬件、操作平台及协议的描述以便不会不必要地在细节上使本发明模糊不清。然而，所属领域的技术人员应了解，尽管指示优选实施例，但详细描述及特定实例仅以图解说明方式而非以限制方式给出。所属领域的技术人员依据本发明将明了在基本发明概念的精神及/或范围内的各种替代、修改、添加及/或重新布置。

[0018] 如本文中所使用，术语“包括(comprises)”、“包括(comprising)”、“包含(includes)”、“包含(including)”、“具有(has)”、“具有(having)”或其任何其它变化形式打算涵盖非排他性包含。举例来说，包括元件列表的过程、产品、物品或设备未必限制于仅那些元件而可包含未明确列出或此过程、物品或设备固有的其它元件。此外，除非明确说明相反的情况，否则“或(or)”是指包含性“或”且不指排他性“或”。举例来说，条件A或B通过以下情况中的任何一者来满足：A为真(或存在)且B为假(或不存在)，A为假(或不存在)且B为真(或存在)，及A与B两者均为真(或存在)。

[0019] 另外，本文中所给出的任何实例或图解说明无论如何不应视为对与所述实例或图解说明一起使用的任何术语的约束、限制或明确定义。而是，这些实例或图解说明应视为关于一个特定实施例进行描述且仅视为说明性的。所属领域的技术人员将了解，这些实例或图解说明与其一起使用的任何术语囊括其它实施例以及可或不可随其给出或在说明书中其它地方给出的其实施方案及调适且所有此些实施例打算包含于所述术语的范围内。指定

此些非限制性实例及图解说明的语言包含但不限制于：“举例来说”、“比如”、“例如”、“在一个实施例中”及诸如此类。

[0020] 可使用任何适合编程语言来实施本文中所描述的本发明的实施例的例程、方法或程序，包含C、C++、Java、汇编语言等。任何特定例程可在单个计算机处理装置或多个计算机处理装置、单个计算机处理器或多个计算机处理器上执行。数据可存储于单个存储媒体中或分布于多个存储媒体中，且可驻存于单个数据库或多个数据库中(或其它数据存储技术)。尽管可以特定次序呈现步骤、操作或计算，但此次序可在不同实施例中改变。在一些实施例中，就在本说明书中将多个步骤展示为循序的来说，可同时执行此些步骤在替代实施例中的某一组合。本文中所描述的操作的顺序可由于另一过程(例如操作系统、内核等)而被中断、暂停或以其它方式控制。所述例程可在操作系统环境中操作或作为独立例程操作。本文中所描述的功能、例程、方法、步骤及操作可在硬件、软件、固件或其任何组合中执行。

[0021] 本文中所描述的实施例可以控制逻辑的形式在软件或硬件或两者的组合中实施。所述控制逻辑可存储于例如计算机可读媒体的信息存储媒体中，因为多个指令经调适以指导信息处理装置来执行各种实施例中所揭示的一组步骤。基于本文中所提供的揭示内容及教示，所属领域的技术人员将了解用以实施本发明的其它方式及/或方法。

[0022] 以软件编程或代码实施本文中所描述的步骤、操作、方法、例程或其部分中的任一者也在本发明的精神及范围内，其中此软件编程或代码可存储于计算机可读媒体中且可由处理器来操作以准许计算机或其它装置执行本文中所描述的步骤、操作、方法、例程或其部分中的任一者。可通过在一个或一个以上计算装置中使用软件编程或代码、通过使用专用集成电路(ASIC)、可编程逻辑装置、现场可编程门阵列等等来实施本发明。

[0023] “计算机可读媒体”可为可含有、存储、传递、传播或输送用于由指令执行系统、设备、系统或装置使用或结合指令执行系统、设备、系统或装置使用的程序的任何媒体。仅以实例方式而非以限制方式，计算机可读媒体可为电子、磁性、光学、电磁、红外或半导体系统、设备、系统、装置、传播媒体或计算机存储器。此计算机可读媒体通常应为机器可读的且包含软件编程或代码，所述软件编程或代码可为人类可读的(例如，源代码)或机器可读的(例如，对象代码)。非暂时性计算机可读媒体的实例可包含随机存取存储器、只读存储器、硬盘驱动器、数据盒式磁带、磁带、软盘、快闪存储器驱动器、光学数据存储装置、光盘只读存储器及其它适当计算机存储器及数据存储装置。在说明性实施例中，软件组件中的一些或全部组件可驻存于单个服务器计算机上或单独服务器计算机的任何组合上。如所属领域的技术人员可了解，实施本文中所揭示的实施例的计算机程序产品可包括存储可在计算环境中由一个或一个以上处理器转译的计算机指令的一个或一个以上非暂时性计算机可读媒体。

[0024] “处理器”包含处理数据、信号或其它信息的任何软件系统、机构或组件。处理器可包含具有通用中央处理单元、多个处理单元、用于实现功能性的专用电路的系统或其它系统。

[0025] 根据各种实施例，将安全签名位添加到如RF跳码发射的数据发射中以检验发射器或收发器单元的真实性及原始性。结合基于无线接入的跳码发射使用安全签名位帮助增加数据发射的安全性而无需切换到更复杂的算法且无涉及所述算法的例如较长数据发射要求的次要问题。

[0026] 根据各种实施例，无线控制接入跳码系统可使用两个独立加密密钥、单个对称块密码加密及CRC计算在仅使RF数据包大小增加不到10%的同时产生安全数位签名。

[0027] 更特定来说，为了减少改进安全性所需要的额外数据位的数目，根据一些实施例的系统利用16位CRC计算，但接着并非仅发送未加密的结果，而是编码器通过使用例如KeeLoq解密算法的解密算法及称作签名密钥(SKEY)的第二64位解密密钥使结果模糊不清。32位跳码或滚动码与16位CRC值的混合也帮助增加安全性，因为现在需要确定两个64位密钥才允许安全性系统工作。

[0028] 现在转到图式，且特别关注图1，展示示范性无线进入系统的图式，且所述示范性无线进入系统由参考编号10大体识别。无线进入系统10实施包含远程发射器12及基站接收器18的无线接入系统。

[0029] 在所图解说明的实施例中，远程发射器12包含一个或一个以上射频(RF)发射器或收发器14及实施根据各种实施例的加密系统的一个或一个以上控制器16。控制器16可实施为包含或配置有加密控制模块17的任何装置或处理器。举例来说，可使用运行适合软件的Microchip微控制器来实施控制器16。然而，可使用其它控制器或处理器。在操作中，控制器16的加密控制模块17对发送到基站接收器18的控制信号进行加密。远程发射器12可进一步配备有用于选择(举例来说)一个或一个以上锁定或解锁功能的一个或一个以上用户输入。

[0030] 基站接收器18可同样包含接收器或收发器20及控制器22。控制器22可实施为包含或配置有解密控制模块23的任何装置或处理器。举例来说，可使用运行适合软件的Microchip微控制器来实施控制器22。然而，可使用其它控制器或处理器。在操作中，控制器22的解密模块23对来自远程发射器12的信号进行解密。

[0031] 基站接收器18可进一步与受控制装置24通信。通常，所述装置实施为锁(例如汽车锁)或电机(例如用于自动车库门的电机)。受控制装置24接收来自基站接收器18的包含(举例来说)用以打开或关闭(或锁定或解锁)的指令的控制信号。

[0032] 如下文将更详细地描述，各实施例提供一种跳码方案，其集成安全签名技术以使用相同安全性算法增加系统级安全性而超过常规跳码系统。安全签名可使用于例如车库开门器或其它无钥匙进入系统的无线接入系统中。额外安全签名位提供在不切换到另一更复杂加密算法的情况下增加整体滚动码跳码系统的级安全性的方式。另外，这些额外安全签名数据位的利用可添加某种保护水平以抵御由第三方对发射器进行不期望的复制。

[0033] 图2图解说明根据一些实施例的示范性码字发射。在所图解说明的实施例中，码字发射200包含未经加密部分204及经加密部分206。在所图解说明的实施例中，码字200为由72个发射位构成的码字。固定代码或未经加密部分204含有28位装置序列号208。经加密部分206含有12位安全签名码210与32位跳码或滚动码212的组合，32位跳码或滚动码212由24位同步计数器214以及4位功能码及用户定义的位中的4个位213构成。在一些实施例中，码字200可包含计数器、计时器或伪随机值、功能值或用户定义的位中的任一者或全部。

[0034] 现在转到图3，展示图解说明根据实施例的由加密控制模块实施的示范性无线接入处理100的图式。注意，处理100图解说明发射侧；针对接收侧将需要类似对应处理。

[0035] 如下文将更详细阐释，处理100包含跳码及签名密钥的应用。在一些实施例中，所述跳码实施为使用传统32位块密码102的跳码部分101，传统32位块密码102使用64位加密密钥(EKEY)104。在所图解说明的实施例中，这些第一32个位内所含有的信息为种子106，其

由24位同步计数器112、4位功能码108及4个用户定义的位110构成。

[0036] 用于每一发射器12(图1)的64位加密密钥104(图3)对于所述发射器来说是唯一的。密钥104可从64位制造商代码及装置的唯一28位序列号导出。此64位制造商代码应受到良好保护且在可能时随时间规律地改变。

[0037] 在所图解说明的实施方案中,用于同步计数器112的位数目为24个位而非传统KeeLoq系统中所使用的16个位,以将计数器组合的数目从65,536增加到16,777,216。计数器值的数目的此增加帮助防止选择性发射捕获技术。在一些实施例中,还可在产生编程期间为发射器指派随机开始计数器值以更佳地利用大计数器空间。

[0038] 8位功能/鉴别码可含有4个按钮信息位108以及4个客户可配置恒定位110。这些位可在解密后验证检查期间使用且也最终用于识别需要何种按钮或功能动作。举例来说,所述功能可为打开或关闭一个或一个以上锁。可将特定锁指派给多按钮控制器上的个别按钮。

[0039] 接着,应用所得32位跳码114以产生16位CRC116。举例来说,如在120处所展示,将32位跳码114分离成(分别)上部16位块122及下部16位块124。接着,对上部块122及下部块124进行“异或”运算126以产生16位CRC116。

[0040] 在一些实施例中,从16位CRC116导出安全签名。特定来说,在一些实施例中,16位CRC116的下部12个位用于安全签名130。安全签名130连同跳码114的上部20个位132一起用作第二32位种子134。代替标准64位装置加密密钥,使用称作安全签名密钥(SKEY)138的不同64位密钥且将其应用于解密算法136。SKEY138对于所有装置来说可为相同的或对每一装置来说为唯一的-使其唯一将添加每一发射器的额外安全性。可以任何方便方式(例如由制造商或客户)提供SKEY138。

[0041] 有利地,可使得用于利用额外12位安全签名位的步骤对于特定制造商的发射器来说为极特定的。任何建立想要与特定系统码兼容的发射器的人员将需要遵循确切相同的计算步骤才起作用。可使用介于从简单CRC检查和计算到使用例如SHA-1等较复杂安全杂凑算法的范围内的各种算法方案来产生这些额外签名位130。

[0042] 返回到图3,解密算法136的输出为第二32位跳码142。接着,将32位跳码142(具有嵌入式安全签名)及跳码114的下部12个位144应用于44位跳码146。最终,将28位序列号140添加到44位跳码146以产生发射码字148,其包含序列号140、安全签名130及32位跳码142。

[0043] 现在转到图4,展示图解说明根据特定实施例的示范性系统操作的流程图400。首先,(步骤402),提供32位种子并使用跳码及第一加密密钥对所述种子进行加密。如上文所述,所述种子可包含计数器位及用户提供的代码或对应于一个或一个以上命令或指令的命令位。所述加密密钥可(举例来说)由远程控制器的制造商提供。接着,可提供所得的第一跳码以供用作循环冗余检查和(CRC)(步骤404)以导出签名。在一个实施例中,安全签名为从16位CRC导出的12位安全签名。

[0044] 接着,将安全签名及跳码的预定位与第二密钥一起使用(步骤406)且使用解密算法(对应于加密算法)及称作签名密钥的第二密钥来解密安全签名及跳码的预定位。接着,将解密算法的输出、预定经加密位及未经加密序列号应用于发射码字(步骤408)。在一些实施例中,所述码字可进一步包含来自第一跳码的预定数目个位。

[0045] 在基站接收器处接收所得码字(步骤410),所述基站接收器对所述码字进行解密

(步骤412)。由基站接收器读取命令指令且所述基站接收器实施所述命令(步骤414)。

[0046] 如上文所述,安全接入发射器的一些实施方案可采用Microchip微控制器。然而,可使用其它微控制器。此外,注意,加密及解密算法可以各种排列使用。因此,所述图仅为示范性的。

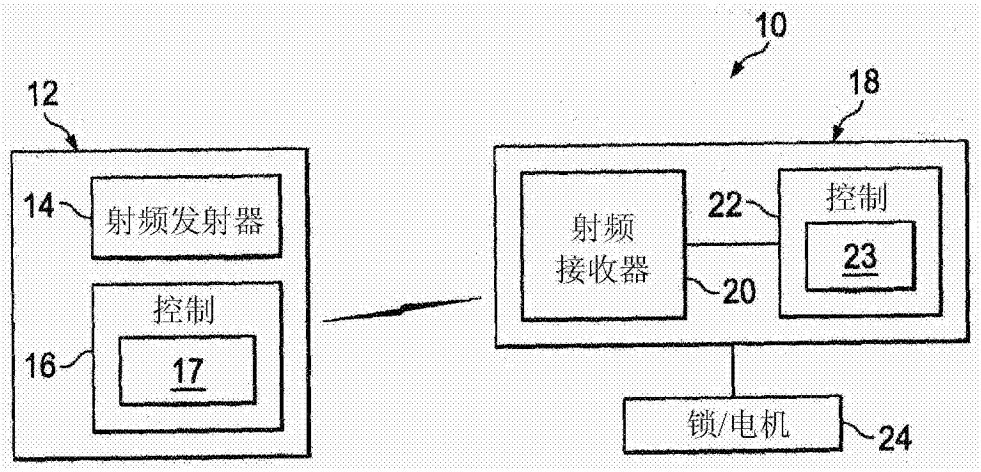

10
12
18
14
射频发射器
控制
16
17
射频
接收器
22
控制
23
20
锁/电机
24

图1

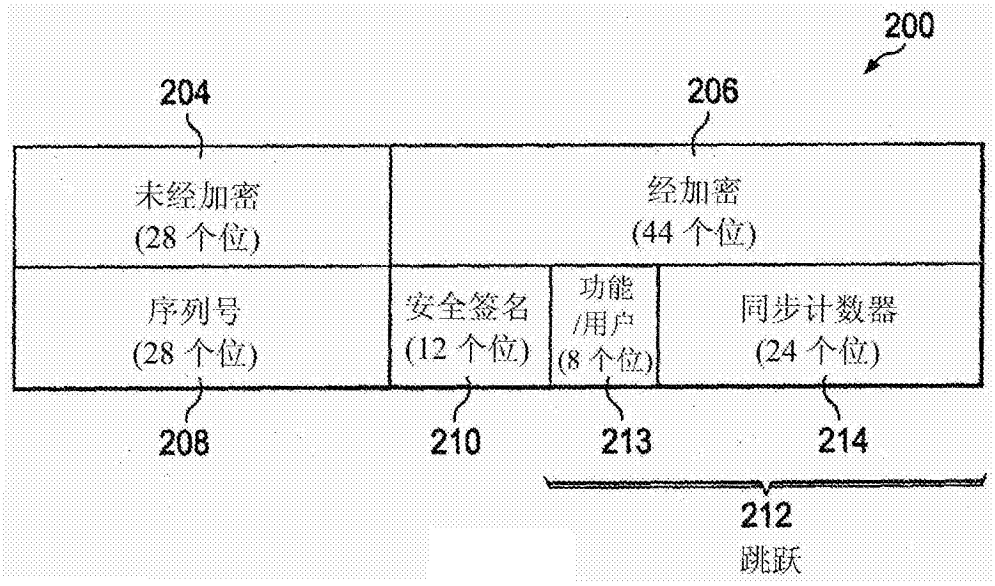

200
204
206
未经加密
(28 个位)
经加密
(44 个位)
序列号
(28 个位)
安全签名
(12 个位)
功能
/用户
(8 个位)
同步计数器
(24 个位)
208
210
213
214
212
跳跃

图2

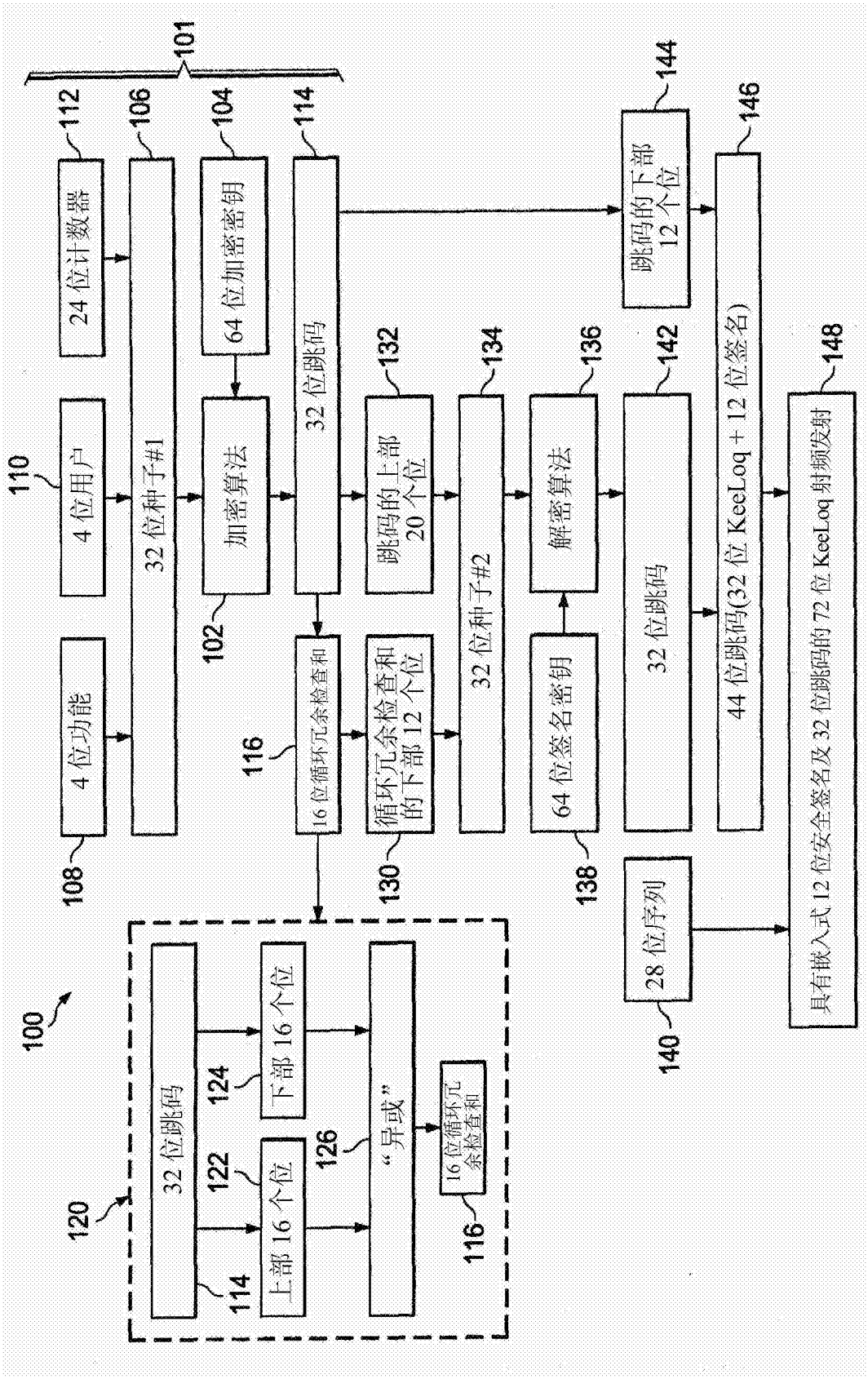

100
101
110
112 24 位计数器
106 32 位种子#1
104 64 位加密密钥
114 32 位跳码
4 位用户
4 位功能
108
102 加密算法
116 16 位循环冗余检查和
132 跳码的上部 20 个位
130 循环冗余检查和的下部 12 个位
134 32 位种子#2
136 解密算法
64 位签名密钥
138
120
32 位跳码
122 上部 16 个位
124 下部 16 个位
126 “异或”
16 位循环冗余检查和
116
142 32 位跳码
144 跳码的下部 12 个位
146 44 位跳码(32 位 KeeLoq + 12 位签名)
140 28 位序列
148 具有嵌入式 12 位安全签名及 32 位跳码的 72 位 KeeLoq 射频发射

图3

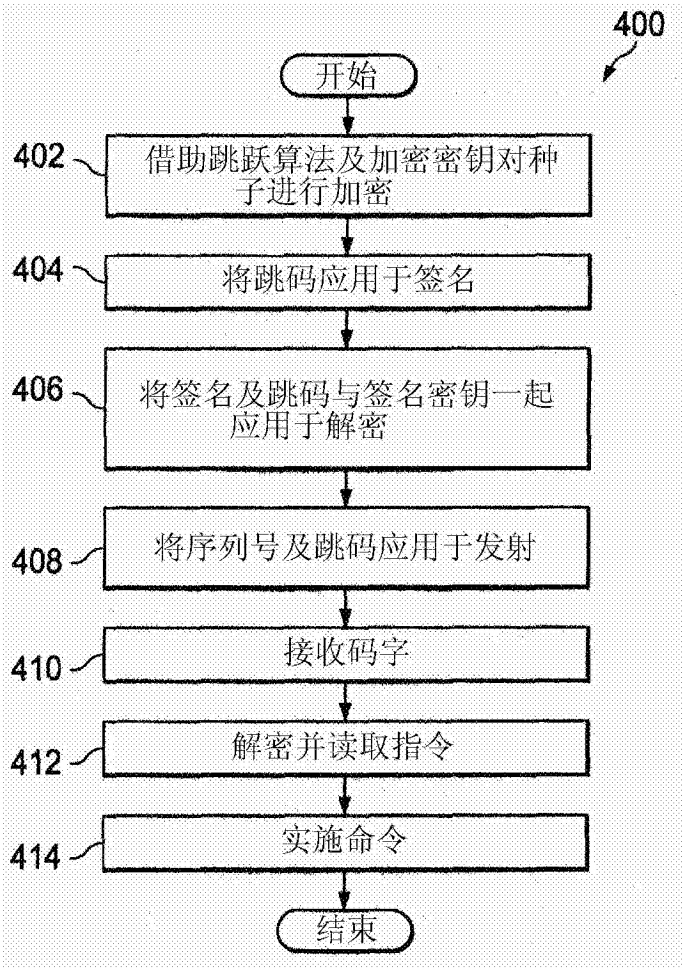

400
开始
402
借助跳跃算法及加密密钥对种子进行加密
404
将跳码应用于签名
406
将签名及跳码与签名密钥一起应用于解密
408
将序列号及跳码应用于发射
410
接收码字
412
解密并读取指令
414
实施命令
结束

图4