(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 103430478 B
(45)授权公告日 2016.08.24

(21)申请号 201280012112.8
(22)申请日 2012.01.10
(30)优先权数据
10-2011-0002474 2011.01.10 KR
(85)PCT国际申请进入国家阶段日
2013.09.06
(86)PCT国际申请的申请数据
PCT/KR2012/000236 2012.01.10
(87)PCT国际申请的公布数据
WO2012/096496 EN 2012.07.19
(73)专利权人 三星电子株式会社
地址 韩国京畿道
(72)发明人 白令教 姜贤贞
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 邵亚丽
(51)Int.Cl.
H04L 9/14(2006.01)
H04W 12/08(2006.01)
(56)对比文件
US 2009307496 A1,2009.12.10,
US 2009305673 A1,2009.12.10,
CN 101203025 A,2008.06.18,
审查员 欧阳洁

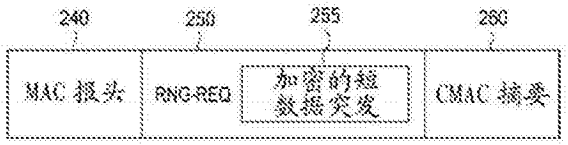
权利要求书3页 说明书9页 附图5页

(54)发明名称

用于在无线通信系统中加密短数据的方法和设备

(57)摘要

一种方法及设备能够在无线通信系统中加密短数据。当终端在空闲模式下生成短数据突发时,所述设备使用从与在终端和基站(BS)之间的安全性关联(SA)相关的授权密钥(AK)得到的基于密码的消息认证码(CMAC)-业务加密密钥(TEK)预密钥来生成TEK。利用与上行链路CMAC PN(CMAC-PN_U)一致的分组号(PN)构建一随机数(nonce),其中所述CMAC-PN_U与携带短数据突发的测距请求(RNG-REQ)消息一起发送。使用所述TEK和所述随机数加密所述短数据突发。



CN 103430478 B

1.一种用于在无线通信系统中的终端上加密短数据的方法,所述方法包括:

在空闲模式下生成短数据突发;

根据从授权密钥(AK)得到的基于密码的消息认证码(CMAC)-业务加密密钥(TEK)预密钥来生成TEK;

由所述终端根据具有与将利用测距请求(RNG-REQ)消息来发送的上行链路CMAC PN(CMAC-PN_U)相同的值的分组号(PN)构建一随机数;

根据所述TEK和所述随机数加密所述短数据突发;

生成包括MAC报头、加密的短数据突发和CMAC摘要的介质访问控制(MAC)协议数据单元(PDU);并且

向BS发送所述MAC PDU。

2.如权利要求1所述的方法,其中,所述测距请求(RNG-REQ)消息包括加密的短数据突发,以及所述CMAC摘要包括所述上行链路CMAC PN

(CMAC-PN_U)。

3.如权利要求2所述的方法,其中,所述测距请求(RNG-REQ)消息包括:测距目的指示字段,其指示发送所述测距请求(RNG-REQ)消息以用于空闲模式位置更新;和CMAC指示符,其指示所述测距请求(RNG-REQ)消息是否受CMAC保护;以及加密的短数据突发。

4.如权利要求3所述的方法,其中,所述测距请求(RNG-REQ)消息包括指示包含在所述测距请求(RNG-REQ)消息中的所述短数据突发是否被加密的加密指示符。

5.如权利要求1所述的方法,其中,所述随机数包括所述短数据突发的长度、站标识符(STID)、流ID(FID)、预定数量的'0'和所述上行链路CMACPN(CMAC-PN_U)。

6.如权利要求1所述的方法,还包括:

通过截短在初始网络进入期间获取的主会话密钥(MSK)来生成成对主密钥(PMK);

使用所述PMK、所述终端的地址和所述BS的ID,对于所述终端和所述BS之间的安全关联(SA)生成AK;并且

使用所述AK生成所述CMAC-TEK预密钥,

其中,TEK生成包括使用所述CMAC-TEK预密钥、所述终端和所述BS之间的所述SA的SA标识符(SAID)和用于所述TEK的TEK计数器值来生成所述TEK,以及

其中,预设所述SAID和所述TEK计数器值。

7.如权利要求1所述的方法,其中,所述短数据突发是短消息服务(SMS)载荷。

8.一种用于在无线通信系统中的基站(BS)上解密短数据的方法,所述方法包括:

从终端接收包括介质访问控制(MAC)报头、加密的短数据突发和基于密码的消息认证码(CMAC)摘要的介质访问控制(MAC)协议数据单元(PDU);

根据从授权密钥(AK)得到的CMAC-业务加密密钥(TEK)预密钥来生成TEK;

根据具有与在所述消息认证码(CAMC)摘要中包含的上行链路CMACPN(CMAC-PN_U)相同的值的分组号(PN)构建一随机数;并且

根据所述TEK和所述随机数解密加密的短数据突发。

9.如权利要求8所述的方法,其中,所述MAC PDU包括测距请求(RNG-REQ)消息,所述测距请求(RNG-REQ)消息包括加密的短数据突发,以及所述消息认证码(CMAC)摘要包括所述上行链路CMAC PN(CMAC-PN_U)。

10.如权利要求9所述的方法，其中，所述测距请求(RNG-REQ)消息包括：测距目的指示字段，其指示发送所述测距请求(RNG-REQ)消息以用于空闲模式位置更新；和CMAC指示符，其指示所述测距请求(RNG-REQ)消息是否受CMAC保护；以及加密的短数据突发。

11.如权利要求9所述的方法，其中，所述测距请求(RNG-REQ)消息包括：加密指示符，其指示包括在所述测距请求(RNG-REQ)消息中的短数据突发是否被加密。

12.如权利要求8所述的方法，其中，所述随机数包括所述短数据突发的长度、站标识符(STID)、流ID(FID)、预定数量的0以及所述上行链路CMACPN(CMAC-PN_U)。

13.如权利要求8所述的方法，还包括：

通过将相关于安全关联(SA)获取的主会话密钥(MSK)截短来生成成对主密钥(PMK)；

使用所述PMK、所述终端的地址和所述BS的ID，对于所述终端和所述BS之间的所述SA生成所述AK；并且

使用所述AK生成所述CMAC-TEK预密钥，

其中，TEK生成包括使用所述CMAC-TEK预密钥、所述终端和所述BS之间的所述SA的SA标识符(SAID)和用于所述TEK的TEK计数器值来生成所述TEK，并且

其中，预设所述SAID和所述TEK计数器值。

14.如权利要求8所述的方法，其中，所述短数据突发是短消息服务(SMS)载荷。

15.一种用于在无线通信系统中加密短数据的终端设备，所述终端设备包括：

生成器，被配置为在空闲模式中生成短数据突发；

加密器，被配置为根据从授权密钥(AK)得到的基于密码的消息认证码(CMAC)-业务加密密钥(TEK)预密钥来生成TEK，根据具有与将利用测距请求(RNG-REQ)消息来发送的上行链路CMAC PN(CMAC-PN_U)相同的值的分组号(PN)构成一随机数，并且根据所述TEK和所述随机数加密所述短数据突发；以及

发送器，被配置为生成包括MAC报头、加密的段数据突发和CMAC摘要的介质访问控制(MAC)协议数据单元(PDU)，并且向BS发送所述MACPDU。

16.如权利要求15所述的终端设备，其中，所述测距请求(RNG-REQ)消息包括加密的短数据突发，以及所述CMAC摘要包括所述上行链路CMACPN(CMAC-PN_U)。

17.如权利要求16所述的终端设备，其中，所述测距请求(RNG-REQ)消息包括：测距目的指示字段，其被配置为指示发送所述测距请求(RNG-REQ)消息以用于空闲模式位置更新；和CMAC指示符，其被配置为指示所述测距请求(RNG-REQ)消息是否受CMAC保护；以及加密的短数据突发。

18.如权利要求16所述的终端设备，其中，所述测距请求(RNG-REQ)消息包括被配置为指示包含在所述测距请求(RNG-REQ)消息中的所述短数据突发是否被加密的加密指示符。

19.如权利要求15所述的终端设备，其中，所述随机数包括所述短数据突发的长度、站标识符(STID)、流ID(FID)、预定数量的‘0’和所述上行链路CMAC PN(CMAC-PN_U)。

20.如权利要求15所述的终端设备，还包括：控制器，被配置为通过截短在初始网络进入期间获取的主会话密钥(MSK)来生成成对主密钥(PMK)，使用所述PMK、所述终端的地址和所述BS的ID，对于所述终端和所述BS之间的安全关联(SA)生成所述AK，并且使用所述AK生成所述CMAC-TEK预密钥，

其中，通过使用所述CMAC-TEK预密钥、所述终端和所述BS之间的所述SA的SA标识符

(SAID)和用于所述TEK的TEK计数器值来生成所述TEK,并且

其中,预设所述SAID和所述TEK计数器值。

21.如权利要求15所述的终端设备,其中,所述短数据突发是短消息服务(SMS)载荷。

22.一种用于在无线通信系统中解密短数据的基站(BS)设备,所述BS设备包括:

接收器,被配置为从终端接收包括介质访问控制(MAC)报头、加密的短数据突发和消息认证码(CMAC)摘要的介质访问控制(MAC)协议数据单元(PDU);

解密器,被配置为根据从授权密钥(AK)得到的CMAC-业务加密密钥(TEK)预密钥来生成TEK,根据具有在消息认证码(CMAC)摘要中包含的上行链路CMAC PN(CMAC-PN_U)相同的值的PN构建一随机数,并且根据所述TEK和所述随机数解密加密的短数据突发。

23.如权利要求22所述的BS设备,其中,所述MAC PDU包括测距请求(RNG-REQ)消息,所述测距请求(RNG-REQ)消息包括加密的短数据突发,以及所述消息认证码(CMAC)摘要包括所述上行链路CMAC PN(CMAC-PN_U)。

24.如权利要求23所述的BS设备,其中,所述测距请求(RNG-REQ)消息包括:测距目的指示字段,被配置为指示发送所述测距请求(RNG-REQ)消息以用于空闲模式位置更新;CMAC指示符,被配置为指示所述测距请求(RNG-REQ)消息是否受CMAC保护;和加密的短数据突发。

25.如权利要求23所述的BS设备,其中,所述测距请求(RNG-REQ)消息包括:加密指示符,被配置为指示是否加密包括在所述测距请求(RNG-REQ)消息中的短数据突发。

26.如权利要求22所述的BS设备,其中,所述随机数包括所述短数据突发的长度、站标识符(STID)、流ID(FID)、预定数量的0以及所述上行链路CMAC PN(CMAC-PN_U)。

27.根据权利要求22所述的BS设备,还包括:控制器,被配置为通过将相关于安全关联(SA)获取的主会话密钥(MSK)截短来生成成对主密钥(PMK),使用所述PMK、所述终端的地址和所述BS的ID,对于所述终端和所述BS之间的所述SA生成所述AK;并且使用所述AK生成所述CMAC-TEK预密钥,

其中,通过使用所述CMAC-TEK预密钥、所述终端和所述BS之间的所述SA的SA标识符(SAID)和用于所述TEK的TEK计数器值来生成所述TEK,以及

其中,预设所述SAID和所述TEK计数器值。

28.如权利要求22所述的BS设备,其中,所述短数据突发是短消息服务(SMS)载荷。

用于在无线通信系统中加密短数据的方法和设备

技术领域

[0001] 本发明涉及无线通信系统，更具体地，本发明涉及用于加密短数据突发的方法和设备。

背景技术

[0002] 诸如码分多址(CDMA)、第三代合作项目(3GPP)长期演进(LTE)系统、微波接入全球互操作性(WiMAX)系统等之类的蜂窝无线通信系统向移动站(MS)提供多种服务。计算机、电子和通信技术的急剧发展是通过无线通信网络提供多种多样的无线通信服务背后的驱动力量。最基本的无线通信服务是无线语音呼叫服务，其使得MS用户能够不管时间和地点而无线地进行语音呼叫。还提供无线因特网服务，这使得用户能够在用户正在移动的同时在任何地点通过无线通信网络经由因特网进行数据通信。

[0003] 特别是，短消息服务(SMS)无论接收MS的通信状态都可在MS之间(换言之，在空闲模式下的MS之间)传递有限长度的文本消息。通常，SMS在液晶屏幕上将文本消息限制为大约80字节。现在，从个人使用到商务使用，SMS的使用率迅猛上升。除了在个人之间的简单消息交换之外，SMS最近发现了其在群发消息、调度消息传输、电子邮件接收提醒、个人信用信息管理、金融信息提醒等中的大范围的使用。

[0004] SMS的增长的使用和重要性增加了SMS安全性的必要性。特别是，当文本消息携带个人信用信息或金融信息时，SMS安全性非常重要。因此，存在对于用于加密由终端发送的短数据突发以便保护SMS安全性的特定技术的需求。

发明内容

[0005] 技术问题

[0006] 为了解决现有技术的上述不足，首要目标是至少提供以下优点。

[0007] 因此，本公开的实施例的一个方面是提供用于在无线通信系统中加密在空闲模式中发送的短数据的方法和设备。

[0008] 本公开的实施例的另一方面是提供用于在无线通信系统中加密由空闲模式的终端发送的短数据的方法和设备。

[0009] 本公开的实施例的又一方面是提供用于在无线通信系统中加密要封装到测距请求(RNG-REG)消息中的短数据的方法和设备。

[0010] 技术方案

[0011] 根据本公开一实施例，提供一种用于在无线通信系统中的终端上加密短数据的方法，其中，在空闲模式中生成短数据突发，使用从与在终端和基站(BS)之间的安全性关联(SA)相关的授权密钥(AK)得到的基于密码的消息认证码(CMAC)-业务加密密钥(TEK)预密钥来生成TEK，其中，通过在初始网络进入期间的认证而提前获取所述AK，利用与上行链路CMAC PN(CMAC-PN_U)一致的分组号(PN)构造一随机数(nonce)，其中所述CMAC-PN_U与携带所述短数据突发的测距请求(RNG-REQ)消息一起发送，使用所述TEK和所述随机数来加密所

述短数据突发，通过将MAC报头和用于整体性保护的CMAC摘要附加到携带已加密短数据突发的RNG-REQ消息来生成介质访问控制(MAC)协议数据单元(PDU)，并且以无线电报信号向所述BS发送所述MAC PDU。所述CMAC-PN_U包含在所述CMAC摘要中。

[0012] 根据本公开另一实施例，提供一种用于在无线通信系统中的BS上解密短数据的方法，其中，从在空闲模式中的终端接收包括包含已加密的短数据突发的测距请求(RNG-REQ)消息、MAC报头和用于整体性保护的CMAC摘要的MAC PDU，使用从与在所述终端和所述BS之间的SA相关的AK得到的CMAC-TEK预密钥来生成TEK，利用与和所述RNG-REQ消息一起发送的上行链路CMAC PN(CMAC-PN_U)一致的PN构造一随机数，并且使用所述TEK和所述随机数来解密所述已加密短数据突发。所述CMAC-PN_U包含在所述CMAC摘要中。

[0013] 根据本公开另一实施例，提供一种用于在无线通信系统中加密短数据的终端设备，其中，生成器在空闲模式中生成短数据突发，加密器使用从与在终端和BS之间的SA相关的AK得到的CMAC-TEK预密钥来生成TEK，其中通过在初始网络进入期间的认证而提前获取所述AK，利用与上行链路CMAC PN(CMAC-PN_U)一致的PN构造一随机数，其中该CMAC-PN_U与携带所述短数据突发的RNG-REQ消息一起发送，并且使用所述TEK和所述随机数来加密所述短数据突发，以及发送器通过向携带已加密短数据突发的RNG-REQ消息附加MAC报头和用于整体性保护的CMAC摘要来生成MAC PDU，并且以无线电信号向所述BS发送所述MAC PDU。所述CMAC-PN_U包含在所述CMAC摘要中。

[0014] 根据本公开又一实施例，提供一种用于在无线通信系统中解密短数据的BS设备，其中，接收器从在空闲模式中的终端接收包括包含已加密短数据突发的RNG-REQ消息、MAC报头和用于整体性保护的CMAC摘要的MAC PDU，以及解密器使用从与在终端和BS之间的SA相关的AK得到的CMAC-TEK预密钥来生成TEK，用与和RNG-REQ消息一起发送的上行链路CMAC PN(CMAC-PN_U)一致的PN构造一随机数，并且使用所述TEK和所述随机数来解密所述已加密短数据突发。CMAC-PN_U包括在CMAC摘要中。

[0015] 以下在着手本发明的详细描述之前，阐述贯穿此专利文件使用的特定词语和短语的定义可能是有益的：术语“包括”和“包含”及其衍生意味着非限制地包括；术语“或”是包括性的，意味着和/或；术语“与..关联”和“与之关联”及其衍生可以意味着包括、包含在其中、与之互连、包含、包含在其中、连接到或与之连接、耦接到或与之耦接、与之可通信、与之合作、交织、并列、靠近、绑定到或与之绑定、具有、具有..的特性等；并且术语“控制器”意味着控制至少一个操作的任何装置、系统或其部分，这样的装置可以以硬件、固件或软件实现，或者以以上的至少两种的某个组合实现。应注意，与任何特定控制器关联的功能可以是集中式的或分布式的，无论本地或远程。贯穿此专利文件提供特定词语和短语的定义，本领域技术人员应当明白，即使不是在大多数情形下也是很多情况下，这样的定义适用于现有技术，以及如此定义的词语和短语的将来使用。

附图说明

[0016] 为了更完整理解本公开及其优点，现在参考下面结合附图进行的描述，在附图中，相同的附图标记表示相同部分：

[0017] 图1图示了根据本公开实施例的短数据传输；

[0018] 图2A图示了包括测距请求(RNG-REQ)消息的介质访问控制(MAC)协议数据单元

(PDU)的典型格式；

[0019] 图2B图示了根据本公开实施例的包括已加密短数据突发的MAC PDU的格式；

[0020] 图3图示了根据本公开实施例的终端的短数据加密操作；

[0021] 图4图示了根据本公开实施例的基站(BS)的短数据解密操作；

[0022] 图5图示了用于加密短数据的结构的框图；

[0023] 图6A和6B图示了根据本公开实施例的用于生成业务加密密钥(TEK)的过程；

[0024] 图7图示了根据本公开实施例的用于加密短数据的终端；和

[0025] 图8图示了根据本公开实施例的用于解密短数据的BS。

[0026] 贯穿附图，相同附图标记将被理解为指代相同元素、特征和结构。

具体实施方式

[0027] 如下所讨论的图1到图8以及此专利文件中用来描述本公开的原理的各种实施例仅是说明的方式并且不应当理解为以任何方式限制本公开的范围。本领域技术人员将明白本公开的原理可以以任何合适布置的无线通信系统来实现。将不给出公知功能和操作的详细描述，以免模糊了本公开的主题。

[0028] 以符合无线蜂窝通信系统中的电气电子工程师协会(IEEE)802.16e/m标准地执行短消息服务(SMS)操作为前提，给出以下描述。然而，本公开不限于特定通信协议或系统配置，并且因此对于本领域技术人员显然的是，可以在本公开的范围和精神内作出许多修改和变型。

[0029] 图1图示了根据本公开优选实施例的短数据传输。参考图1，基站(BS)110的小区区域内的移动站(MS)120以无线电信号向BS110发送所期望的文本消息，并且BS110向接收终端130发送该文本消息。接收终端130可以是另一蜂窝MS、PC等。在IEEE802.16m标准中，BS110和MS120分别称为高级BS(ABS)和高级MS(AMS)，并且ABS和AMS之间的空中接口称为高级空中接口(AAI)。

[0030] 如果意图发送文本消息的MS正在进行呼叫(即其处于活跃模式)，则文本消息被加密并且在业务消息中发送。替代地，如果MS未正在进行呼叫(即其处于空闲模式)，则文本消息被携带在空闲模式下在没有网络重进入的情况下可发送的消息中(例如在符合IEEE802.16m标准的AAI测距请求(AAI_RNG-REQ)消息中)。类似地，在AAI测距响应(AAI_RNG-RSP)消息中发送对于空闲模式MS的文本消息。

[0031] 当在空闲模式中生成短数据时，终端在用于在无网络重进入的情况进行位置更新的RNG-REQ消息中发送短数据突发(即SMS净载荷)，由此节约能源。

[0032] 图2A图示了包括RNG-REQ消息的介质访问控制(MAC)协议数据单元(PDU)的典型格式。

[0033] 参考图2A，MAC PDU包括MAC报头210、包括RNG-REQ消息的净载荷220和用于错误校验和整体性保护的基于密码的消息认证码(CMAC)摘要230。如果RNG-REQ消息用于SMS传输，则短数据突发225被封装在净载荷220中。CMAC摘要230包括与BS和终端之间的安全性关联(SA)相关的PMK_SN和CMAC-PN_U以及对RNG-REQ消息计算的CMAC值，用于RNG-REQ消息的整体性保护。

[0034] PMK_SN是用于验证RNG-REQ消息的整体性的成对主密钥(PMK)的序列号(SN)。

CMAC-PN_U是在上行链路(UL)上使用的CMAC分组号(PN)。

[0035] 具体地,UL或下行(DL)CMAC PN是UL或DL控制消息的CMAC SN。UL或DL CMAC PN是在UL或DL消息的情形中对于包含CMAC元组或CMAC摘要的每一MAC控制消息而递增的顺序计数器。

[0036] CMAC PN是在BS和MS之间的认证过程中获取的授权密钥(AK)上下文的一部分,对于由CMAC保护的MAC控制消息(诸如,RNG-REQ消息)是唯一的。

[0037] 图2A中所示的MAC PDU格式支持RNG-REQ消息的整体性保护,但是不支持短数据突发225的加密。

[0038] 图2B图示了根据本公开的优选实施例的包括已加密短数据突发的MAC PDU的格式。

[0039] 参考图2B,MAC PDU包括MAC报头240、包括RNG-REQ消息的净载荷250和用于错误校验和整体性保护的CMAC摘要260。特别是,已加密短数据突发225被封装在净载荷250中。如图2A那样,CMAC摘要260包括PMK_SN、CMAC-PN_U以及对RNG-REQ消息计算的CMAC值。

[0040] 依据本公开的实施例,可以以具有计数器码(AES-CTR)加密方案的高级加密标准来加密短数据突发255。AES-CTR是IEEE802.16m标准支持的加密方案中的一种,其中,没有整体性验证地加密文本。即,因为由CMAC摘要260确保整个RNG-REQ消息的整体性,所以可以借助通过AES-CTR加密短数据突发255来最小化MAC PDU的尺寸的改变。

[0041] AES-CTR方案需要输入业务加密密钥(TEK)和随机数N。从使用主会话密钥(MSK)生成的CMAC-TEK预密钥和从MSK得到的AK得到TEK。当初始地访问网络时,即,在网络进入和初始化期间,终端可以在认证步骤中获取MSK。

[0042] 例如,TEK可以通过以下等式得到。

[0043] TEK=Dot16KDF(CMAC-TEK prekay,SAID|COUNTER_TEK=0|TEK,128)

[0044] 其中,Dot16KDF表示预定密钥导出函数,SAID是标识BS和终端之间的SA的SA标识符,并且COUNTER_TEK是用来从相同SAID得到不同TEK的计数值。在替代实施例中,可以预设SAID和COUNTER_TEK。例如,SAID设为0x02,而COUTNER_TEK设为0。基于CMAC-TEK预密钥、SAID=0x02和COUNTER_TEK=0生成的TEK被用于短数据突发255的加密。

[0045] 例如,如表1所示,使用PN构造随机数N。

[0046] [表1]

[0047]

字节数	0 - 1	2 - 3	4 - 9	10 - 12
字段名	短数据突发的长度	STID 和流 ID	预留	EKS 和分组号
内容	短数据突发的长度	STID|FID	0x000000000000	00|CMAC_PN_U

[0048] 参考[表1],随机数的前两个字节用短数据突发的长度来填充。如果站ID(STID)和流ID(FID)尚未被分配给终端的服务流,则STID和FID字段被设为全零(0)。加密密钥序列(EKS)字段用0填充并且用来构建随机数的PN设为与和RNG-REQ消息一起发送的CMAC-PN_U

的值相同的值。使用CMAC-PN_U的原因在于不像业务MAC PDU,RNG-REQ消息不具有PN。

[0049] 在替代实施例中,RNG-REQ消息可以包括加密指示符,其指示是否加密短数据突发255。加密指示符是1位长,其指示是否加密了RNG-REQ消息中封装的短数据突发。以下的[表2]图示了包括加密指示符的RNG-REQ消息的示例格式。

[0050] [表2]

[0051]

字段	尺寸(位)	值/描述	条件
测距目的指示	4	.....0b0011 = 空闲模式 位置更新.....	
CMAC 指示符	1	指示此消息是否由 CMAC 元组被保护 0b0: 未保护 0b1: 已保护	
SMS 加密指示符	1	指示此 SMS 是否被加密 0b0: 未加密 0b1: 已加密	
SMS	可变	最多 140 字节的短消息内容	当存在要发送的 SMS 内容时可以呈现

[0052] 在[表2]中,测距目的指示指示了RNG-REQ消息的目的。如果RNG-REQ消息用来发送短数据突发,测距目的指示则可以设置为0b0011。CMAC指示符是指示RNG-REQ消息是否由CMAC保护的1位字段,并且SMS加密指示符是指示短数据突发是否被加密的1位字段。

[0053] 图3图示根据本公开实施例的终端的短数据加密操作的流程图。

[0054] 参考图3,空闲模式的终端在块302中生成要发送到对端(peer)的短数据突发,并且在块304中确定是否加密所述短数据突发。在示例中,当在初始网络进入期间协商终端的能力时,可以基于相关参数做出确定。在本公开另一实施例中,如果规定总是加密短数据突发,则可以省略块304。在此情况下,过程从块302跳到块306。可以根据所使用的通信标准或系统设计者的选择而确定是否省略块304。

[0055] 如果终端在块304确定不加密短数据突发,则跳到块308。替代地,如果终端在块304确定加密短数据突发,则终端前进到块306。在块306,终端使用在初始网络进入期间要求的授权相关参数(即使用从MSK和MSK得到的AK生成的CMAC-TEK预密钥)生成加密短数据突发所需的TEK,使用包括要在其中封装短数据突发的RNG-REQ消息的MAC PDU的PN构建一随机数,并且使用所述TEK和所述随机数加密短数据突发。PN可以设置为在MAC PDU中包括的CMAC-PN_U。

[0056] 终端在块308确定是否对将在其中封装短数据突发的RNG-REQ消息执行CMAC保护,

这是可选的。可以例如在初始网络进入期间的协商过程中，提前做出块308的确定。如果终端确定要执行CMAC保护，则终端前进到块310，否则，跳到块312。

[0057] 在块310，终端使用CMAC-TEK预密钥生成CMAC密钥，并且从CMAC密钥得到CMAC值，以包括在与RNG-REQ消息一起的、MAC PDU的CMAC摘要中。在块312，终端生成包括已加密的短数据突发并且可选地进一步包括CMAC指示符和SMS加密指示符的RNG-REQ消息，通过向该RNG-REQ消息添加MAC报头和CMAC摘要来构建MAC PDU，并且以无线电信号向BS发送所述MAC PDU。

[0058] 图4是图示根据本公开的实施例的BS的短数据解密操作的流程图。

[0059] 参考图4，BS在块402从空闲模式的终端接收包括RNG-REQ消息的MAC PDU，并且在块404基于在RNG-REQ消息中包括的CMAC指示符确定RNG-REQ消息是否是受CMAC保护的。如果CMAC指示符指示RNG-REQ消息是受CMAC保护的，则BS前进到块406。否则，BS在块418丢弃RNG-REQ消息。

[0060] 在块406，BS根据在RNG-REQ消息中包括的信息从认证器获取AK上下文以便认证终端。如果BS已经具有与该终端相关的AK上下文，则可以不进行块406。在块408，BS随后使用从AK得到的CMAC-TEK预密钥生成CMAC密钥，并且使用CMAC密钥验证RNG-REQ消息的CMAC。更具体地，BS使用CMAC密钥对RNG-REQ消息计算CMAC值，并且比较所计算得到的CMAC值与附加到RNG-REQ消息的CMAC摘要中设置的CMAC值。

[0061] 如果CMAC值相等，则BS在块410确定RNG-REQ消息的CMAC值是有效的。如果RNG-REQ消息的CMAC值无效，则BS在块418丢弃RNG-REQ消息。替代地，如果RNG-REQ消息的CMAC值有效，则BS在块412基于RNG-REQ消息中包括的加密指示符确定在RNG-REQ消息中封装的短数据突发是否已被加密。如果加密指示符指示短数据突发未被加密，则BS跳到块416。如果加密指示符指示短数据突发已被加密，则BS前进到块414。在本公开的另一实施例中，如果规定总是加密短数据突发，则RNG-REQ消息不包括加密指示符并且因此BS直接前进到块414而不执行块412。

[0062] 在块414，BS使用CMAC-TEK预密钥生成与在终端中用于短数据突发的加密的TEK相同的TEK，使用附加到RNG-REQ消息的CMAC-PN_U构建随机数，并且使用所述TEK和所述随机数解密在RNG-REQ消息中封装的短数据突发。在块416，BS执行包括已加密的短数据突发的显示的处理。

[0063] 可以在终端的初始化期间确定终端是否要加密短数据突发。根据本公开的替代实施例，指示移动发起的(MO)短数据突发的加密的指示符可以包括在由终端在其初始化期间发送的用户站基本能力请求(SBC-REQ)消息中，或者包括在响应于SBC-REQ消息的用户站基本能力响应(SBC-RSP)消息中，其中借助该消息，BS回复终端。在本公开的另一实施例中，指示符可以包括在由终端在网络注册期间发送的注册请求(REG-REQ)消息中，或者包括在BS响应于REG-REQ消息发送到终端的注册响应(REG-RSP)消息。

[0064] 以下的[表3]图示了SBC-REQ/RSP消息或包括MO SNS加密指示符的REG-REQ/RSP消息的示例性格式。

[0065] [表3]

[0066]

字段	尺寸(位)	值/描述	条件
MO(移动发起的)SMS 加密	1	指示 MO SMS 是否可以被加密 0b0: 支持加密 0b1: 不支持加密	

[0067] 现在,将给出用于加密和解密短数据突发的步骤的详细描述。

[0068] 图5是用于通过AES-CTR加密短数据的结构的框图。参考图5,AES-CTR加密模块504加密输入的TEK502。组合器506组合短数据突发508和加密的TEK,由此产生加密的短数据突发510。

[0069] 如上所述,因为基于对BS和终端已知的参数、通过RNG-REQ和RNG-RSP消息交换的参数或可预期的参数生成TEK502,所以相比于加密的业务数据,已加密短数据突发510不与诸如EKS和PN之类的额外净负荷附接。虽然加密了携带业务数据的MAC PDU,但是在本公开的实施例中在生成携带RNG-REQ消息的MAC PDU的处理中仅加密短数据突发。

[0070] 下面将描述用于生成在短数据突发的加密中使用的TEK的过程。

[0071] 图6A和6B图示了根据本公开的实施例的用于生成TEK的过程。

[0072] 参考图6A,在终端的认证期间,从认证、授权和计费(AAA)服务器生成512位的MSK602,并且发送到认证器。终端在认证期间生成与在AAA服务器中生成的MSK相同的MSK。终端和认证器通过将MSK截短(truncate)到160位得到160位PMK604。从MSK602得到PMK604可以表示为:

[0073] PMK=truncate(MSK,160)

[0074] 如果初始认证成功,则BS和终端可以在基于可扩展身份验证协议(EAP)的认证过程中从PMK604得到AK606,并且在它们之间共享该AK606。例如,AK606可以通过以下生成:

[0075] AK=Dot16KDF(PMK,AMS Address|ABSID|"AK",160)

[0076] 其中,AMS Address(AMS地址)可以是终端的MAC地址或MS ID(MSID)。MSID是使用MS的MAC地址作为种子生成的随机值。ABSID是BS的ID。

[0077] 参考图6B,基于AK606生成TEK614。具体地,通过使用AK606执行KDF生成CMAC-TEK预密钥(CMAC-TEK prekey)610。例如,通过以下得到CMAC-TEK预密钥610:

[0078] CMAC-TEK prekey=Dot16KDF(AK,AK_COUNT|"CMAC_TEK prekey",160)

[0079] 其中,AK_COUNT是用来确保不同的CMAC密钥和TEK用于相同的BS-终端对的计数器值。

[0080] 然后,如下使用CMAC-TEK预密钥610来生成128位的TEK614。

[0081] TEKi=Dot16KDF(CMAC-TEK prekey,SAID|COUNTER_TEK=I|"TEK",128)

[0082] 其中,如上所述SAID例如预设为0x02。TEK614(即使用SAID=0x02和COUNTER_TEK=0生成的TEK0)用于短数据突发的加密。

[0083] 此外,可以使用CMAC-TEK预密钥610生成用于上行链路和下行链路的CMAC_KEY_U和CMAC_KEY_D,并且使用CMAC_KEY_U生成附加到RNG-REQ消息的CMAC摘要中的CMAC值(CMAC

value)。例如,如下给出CMAC值:

[0084] CMAC value=Truncate(CMAC(CMAC_KEY_U,AK ID|CMAC_PN|STID|FID|24-bit zero padding(24位的零填充)|ASN.1encoded MAC_Control_Message(ASN.1编码的MAC控制消息)),64)

[0085] 其中,STID是终端的站标识符。如果STID未被分配给终端,则STID可以被设置为'000000000000'。

[0086] AKID标识用于保护消息的AK,例如,如下生成。

[0087] AKID=Dot16KDF(AK,0b0000|PMK SN|AMSID or MS MAC Address(MS MAC地址)|ABSID|"AKID,64)

[0088] 根据AK推导公式,可以使用AMSID或MS MAC地址。

[0089] 再次参考图3和4,在块310,终端使用从CMAC-TEK预密钥得到的CMAC-TEK密钥生成CMAC值,并且与CMAC值一起发送RNG-REQ消息到BS。在块408,BS通过将使用从CMAC-TEK预密钥得到的CMAC密钥生成的CMAC值与附加到RNG-REQ消息的CMAC值进行比较来验证RNG-REQ消息。

[0090] 根据前述实施例的操作可以通过提供存储了与BS和终端中的操作对应的程序代码的存储器来实现。即,BS和终端通过处理器或中央处理器(CPU)从存储器读取程序代码并且执行该程序代码来执行所述操作。具体地,配置BS和终端两者或之一以根据本公开的实施例执行短数据突发加密/解密。

[0091] 图7是根据本公开的实施例的用于加密短数据的终端的框图。虽然分离配置地在图7中示出终端的组件,但是多个组件可以合并成控制器或处理器。

[0092] 参见图7,短数据生成器702产生要发送到对端的短数据突发。加密器704在控制器710的控制下,基于从存储器712接收的授权相关参数加密从短数据生成器702接收的短数据突发。具体地,控制器710根据初步协商或预设规则确定是否加密短数据突发,并且根据该确定控制加密器704。存储器712存储在初始网络进入期间获取的授权相关参数,包括通过控制器712从MSK和AK得到的CMACK-TEK预密钥,并且在控制器712的控制下向加密器704提供CMAC-TEK预密钥。

[0093] 加密器704使用该CMAC-TEK预密钥生成短数据突发的加密所需的TEK,使用包括其中封装了短数据突发的RNG-REQ消息的MAC PDU的PN构建随机数,并且使用所述TEK和所述随机数加密短数据突发。PN可以与在MAC PDU中包括的CMAC-PN_U相同。

[0094] 消息生成器706构建包括由加密器704加密的短数据突发的RNG-REQ消息,并且生成包括具有使用CMAC-TEK预密钥生成的CMAC值的CMAC摘要的MAC PDU。发送器708以无线电信号向BS发送MAC PDU。

[0095] 图8是根据本公开的实施例的用于解密短数据的BS的框图。虽然分离配置地在图8中示出终端的组件,但是多个组件可以合并成控制器或处理器。

[0096] 参考图8,接收器802以无线电信号接收包括RNG-REQ消息的MAC PDU。消息解译器804从自接收器802接收的MAC PDU解析出MAC报头、RNG-REQ消息和CMAC摘要并且解译它们。特别地,消息解译器804在控制器810的控制下解译RNG-REQ消息并且从所述RNG-REQ消息提取短数据突发。

[0097] 解密器806在控制器810的控制下基于从存储器812接收的授权相关参数,解密从

消息解译器804接收的已加密短数据突发。具体地，控制器810根据RNG-REQ消息中包括的加密指示符确定是否对短数据突发进行解密，并且根据该确定控制解密器806。另外，控制器810根据在RNG-REQ消息中包括的信息从认证器获取用于认证终端的AK上下文，基于该AK上下文得到CMAC-TEK预密钥，并且存储该CMAC-TEK预密钥在存储器812中。解密器806使用从存储器812接收的CMAC-TEK预密钥生成与在终端中用于加密短数据突发的TEK相同的TEK，使用附加到RNG-REQ消息的CMAC-PN_U构建一随机数，并且使用所述TEK和所述随机数解密已加密短数据突发。短数据处理器808执行包括在显示器上显示或输出已解密短数据突发的必要操作。

[0098] 现在从以上描述是显而易见的，因为根据本公开加密要从空闲模式的终端发送的短数据，所以终端可以安全地发送重要的信息。具体地，使用在公知加密方案中BS和终端均已知的授权相关参数加密短数据而不使用额外参数。因而，向短数据提供安全性而不增加系统和信令开销。

[0099] 尽管已经用示例性实施例描述了本公开，但是可以向本领域技术人员提出各种改变和修改。本公开意图包括这样的改变和修改，只要落在所附权利要求的范围内。

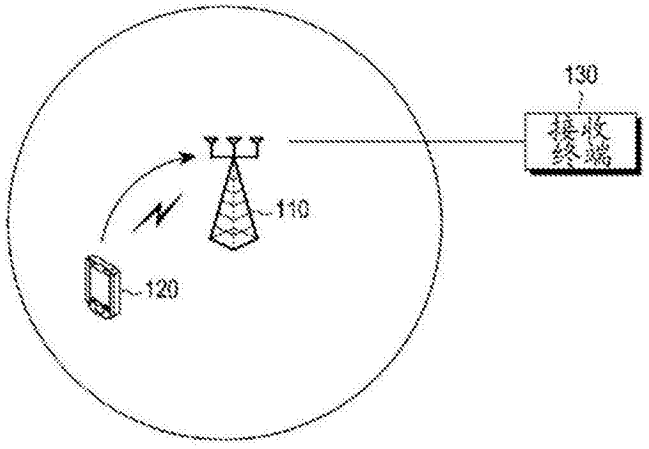

130
接收
终端
110
120

图1

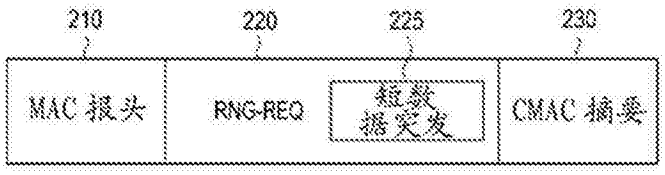

210
220
225
230
MAC 报头
RNG-REQ
短数
据突发
CMAC 摘要

图2A

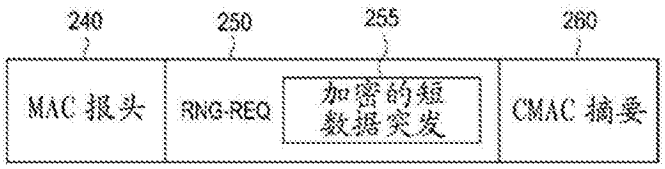

240
250
255
260
MAC 报头
RNG-REQ
加密的短
数据突发
CMAC 摘要

图2B

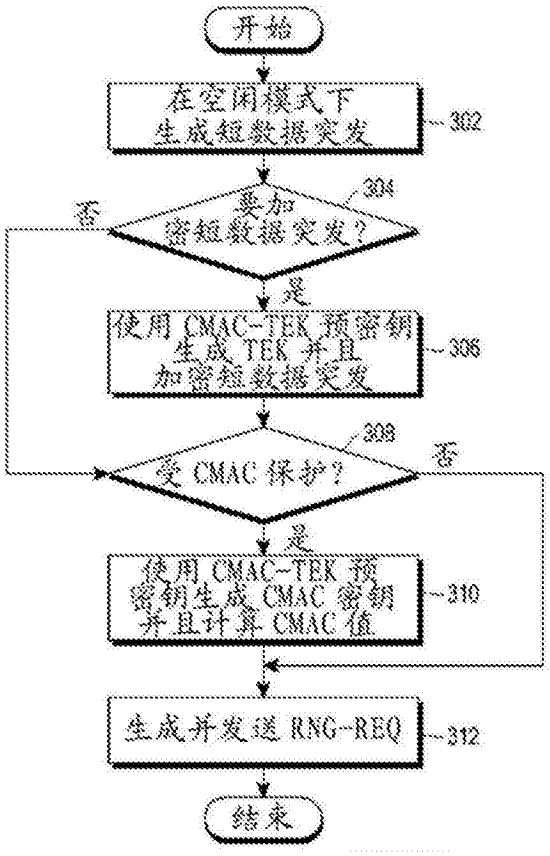

开始
在空闲模式下
生成短数据突发
302
要加
密短数据突发?
304
否
是
使用 CMAC-TEK 预密钥
生成 TEK 并且
加密短数据突发
306
受 CMAC 保护?
308
否
是
使用 CMAC-TEK 预
密钥生成 CMAC 密钥
并且计算 CMAC 值
310
生成并发送 RNG-REQ
312
结束

图3

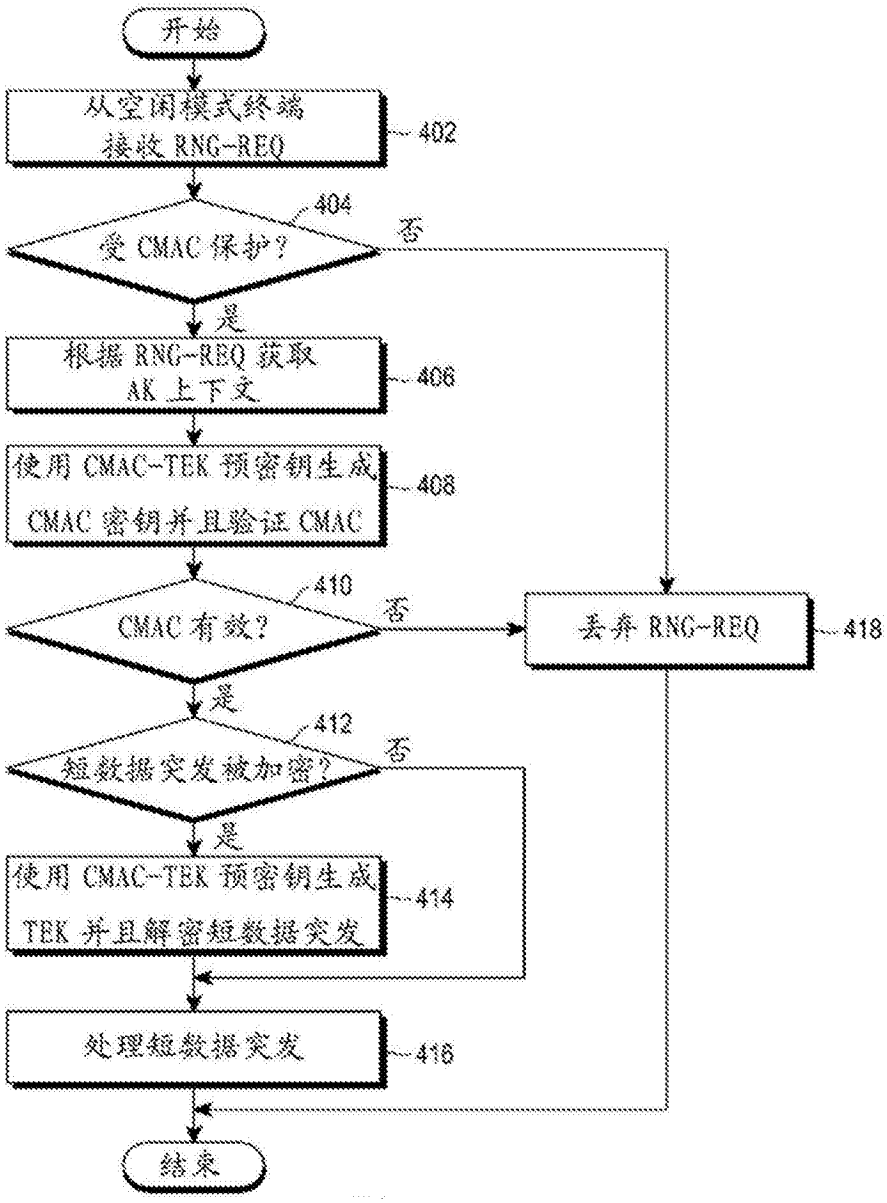

开始
从空闲模式终端
接收 RNG-REQ
402
受 CMAC 保护?
404
否
是
根据 RNG-REQ 获取
AK 上下文
406
使用 CMAC-TEK 预密钥生成
CMAC 密钥并且验证 CMAC
408
CMAC 有效?
410
否
丢弃 RNG-REQ
418
是
短数据突发被加密?
412
否
是
使用 CMAC-TEK 预密钥生成
TEK 并且解密短数据突发
414
处理短数据突发
416
结束

图4

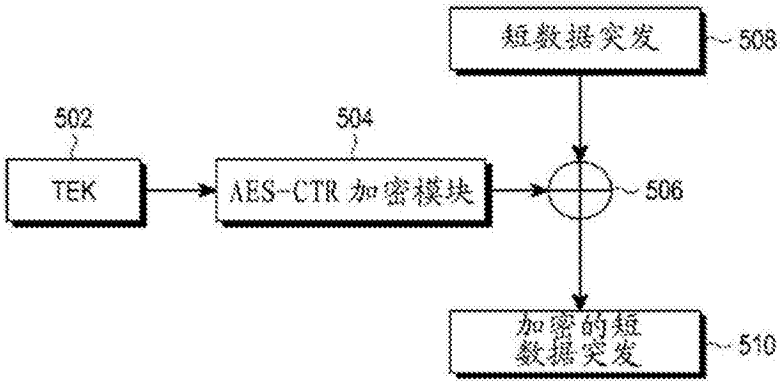

短数据突发
508
502
504
TEK
AES-CTR 加密模块
506
加密的短
数据突发
510

图5

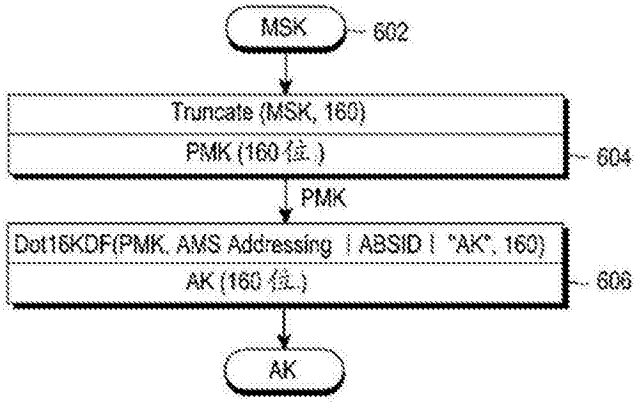

MSK
602
Truncate (MSK, 160)
PMK (160 位)
604
PMK
Dot16KDF(PMK, AMS Addressing | ABSID | "AK", 160)
AK (160 位)
606
AK

图6A

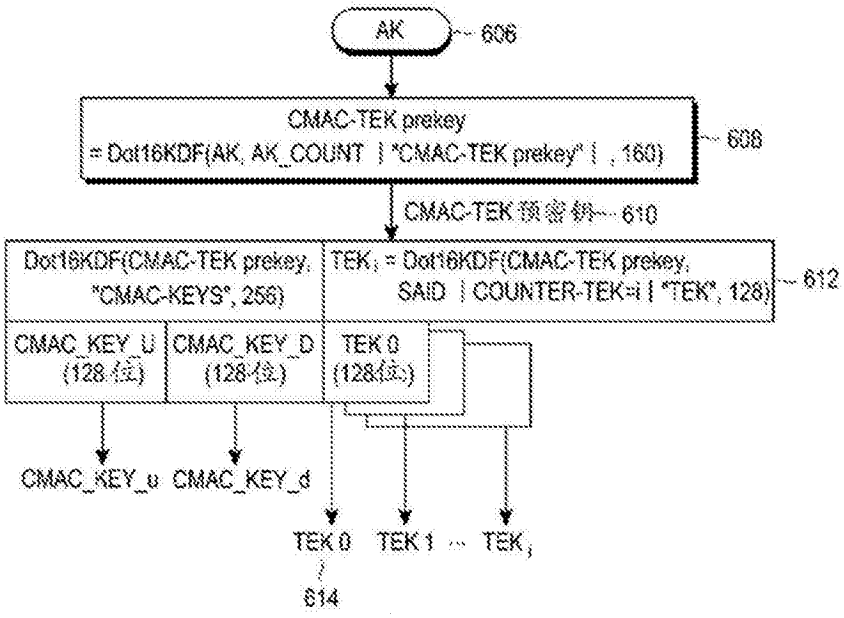

AK
606
CMAC-TEK prekey
= Dot16KDF(AK, AK_COUNT | "CMAC-TEK prekey" | , 160)
608
CMAC-TEK 预密钥
610
Dot16KDF(CMAC-TEK prekey, "CMAC-KEYS", 256)
TEK$_i$ = Dot16KDF(CMAC-TEK prekey, SAID | COUNTER-TEK=i | "TEK", 128)
612
CMAC_KEY_U (128 位)
CMAC_KEY_D (128 位)
TEK 0 (128 位)
CMAC_KEY_u
CMAC_KEY_d
TEK 0
TEK 1
TEK$_i$
614

图6B

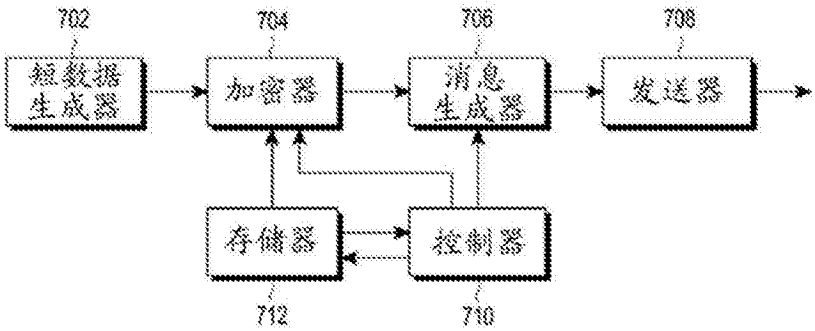

702
短数据生成器
704
加密器
706
消息生成器
708
发送器
存储器
712
控制器
710

图7

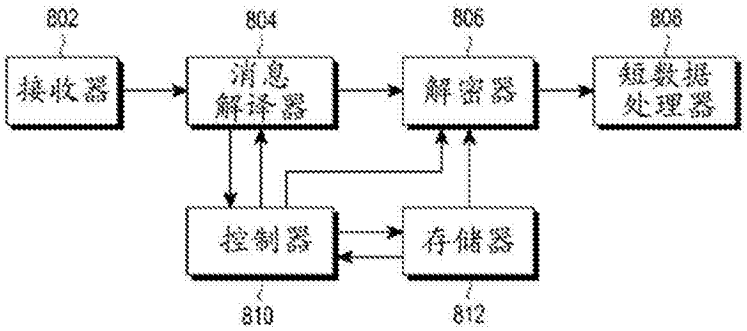


图8