

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.



[12] 发明专利说明书

专利号 ZL 03152635.7

H04L 9/00 (2006.01)

H04L 9/06 (2006.01)

H04K 1/00 (2006.01)

[45] 授权公告日 2009 年 7 月 15 日

[11] 授权公告号 CN 100514904C

[22] 申请日 2003.8.1 [21] 申请号 03152635.7

[30] 优先权

[32] 2002.8.7 [33] KR [31] 46599/02

[73] 专利权人 居里泰尔公司

地址 韩国京畿道

[72] 发明人 崔敬颢 李吉浩 宋文燮 李俊雨

[56] 参考文献

EP0641140 A2 1995.3.1

CN1307771 A 2001.8.8

DE3418571 A 1984.11.22

审查员 张 鑫

[74] 专利代理机构 北京市柳沈律师事务所

代理人 邸万奎 黄小临

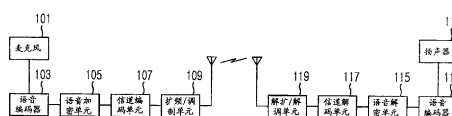
权利要求书 1 页 说明书 6 页 附图 3 页

[54] 发明名称

自动进入无线通信终端的安全通信模式的方法

[57] 摘要

提供一种通过将语音信号的一部分形成为用于尝试安全语音通信的标记，无须改变或预设置传统的无线移动通信系统，即可自动进入可以在发送终端和接收终端之间执行安全的语音通信的方法，和一种用于记录实现该方法的程序的计算机可读记录介质。本发明的方法包括步骤：a) 基于从该无线通信终端的语音编码器输出的语音数据中具有最低产生频率的数据而产生标记；b) 在发送终端，接收来自用户的对于安全通信的请求，并向接收终端发送该标记；和 c) 在该发送终端，基于从该接收终端发送的确认标记进入安全通信模式，并执行与该接收终端之间的安全通信。



1. 一种自动进入无线通信终端的安全通信模式的方法，包括步骤：
 - a) 基于从该无线通信终端的语音编码器输出的语音数据中具有最低产生频率的数据而产生标记；
 - b) 在发送终端，从用户接收对于安全通信的请求，并向接收终端发送该标记；
 - c) 在接收终端，检验是否接收到从发送终端发送的标记，并将确认标记发送至发送终端；
 - d) 在接收终端，进入安全通信模式，并执行与该发送终端之间的安全通信；和
 - e) 在该发送终端，基于从该接收终端发送的确认标记进入安全通信模式，并执行与该接收终端之间的安全通信。
2. 如权利要求 1 所述的方法，其中该从发送终端发送的标记包括具有从所述语音编码器输出的语音分组数据的数据中最低产生频率的数据作为标记首标。
3. 如权利要求 1 所述的方法，其中该从发送终端发送的标记短于从语音编码器输出的数据的最大长度。
4. 如权利要求 3 所述的方法，其中该从发送终端发送的标记包括在用于安全通信的加密算法中使用的密钥。
5. 如权利要求 1 所述的方法，其中在步骤 b)，将该从发送终端发送的标记重复发送预定次数。
6. 如权利要求 5 所述的方法，其中在步骤 b)，当接收到从接收终端发送的确认标记时，停止该从发送终端发送的标记的重复发送。
7. 如权利要求 1 所述的方法，其中所述步骤 c) 包括步骤：
 - f) 检验在发送终端产生并包含在该从发送终端发送的标记中的会话密钥与使用主密钥在接收终端中产生的会话密钥是否匹配。

自动进入无线通信终端的安全通信模式的方法

技术领域

本发明涉及一种无线移动通信终端，并尤其涉及一种用于自动进入安全通信模式以无须改变或预置无线移动通信系统而执行发送终端和接收终端之间的语音加密的方法，和一种用于记录实现该方法的程序的计算机可读记录介质。

背景技术

无线移动通信系统中的已知安全通信技术之一是使用私有密钥加密数据的数据加密标准（DES）。在 DES 中，使用超过 72×10^{15} 个私有密钥。从这多个密钥中随机选择用于每条消息的密钥。正如其他私有密钥加密方法一样，发送和接收终端双方应知道和使用相同的私有密钥。在 DES 技术中，使用 64-比特数据块中的 56 比特作为密钥。可在各种模式中执行该处理，并且该处理应经历 16 次运算。DES 是由 IBM 开发的，并在 1977 年被采纳为联邦标准。DES 在美国国家标准化组织（ANSI）X3.92 和 X3.106 标准以及联邦信息处理标准（FIPS）46 和 81 之中。

然而传统安全通信系统存在缺点，即为了使语音通信安全而需要语音通信安全设备，也就是加密设备。该语音通信安全设备是仅用于防止语音通信被窃听的系统。

用于安全语音通信的另一传统技术是验证语音秘密性技术。在该技术中，将用于尝试安全语音通信的特定消息从发送终端发送到基站，该基站向接收终端发送用于验证的消息，以执行安全语音通信。

然而，该技术也存在问题，即必须在通信系统中预置用于安全语音通信的特定消息。由于该基站得知对于安全语音通信建立了通信信道，所以该通信信道可能成为被攻击的目标。

发明内容

所以，本发明的目的在于提供一种通过将在发送终端和接收终端之间通

信的语音信号的一部分形成一个用于尝试安全语音通信的标记，无须改变无线移动通信系统的传统设置，从正常通信模式进入安全通信模式的方法，和一种用于记录实现该方法的程序的计算机可读记录介质。通过附图、具体实施方式和权利要求，本领域普通技术人员应能理解本发明的其他目的和优点。

根据本发明的一个方面，提供了一种自动进入无线通信终端的安全通信模式的方法，包括步骤：a) 基于从无线通信终端的语音编码器输出的语音数据中具有最低产生频率的数据而产生一个标记；b) 在发送终端，接收来自用户的对于安全通信的请求，并向接收终端发送该标记；c) 在接收终端，检验是否接收到从发送终端发送的标记，并将确认标记发送至发送终端；d) 在接收终端，进入安全通信模式，并执行与该发送终端之间的安全通信；和 e) 在该发送终端，基于从该接收终端发送的确认标记进入安全通信模式，并执行与该接收终端之间的安全通信。

根据本发明的另一方面，提供了一种用于记录程序的计算机可读记录介质，该程序实现用于自动进入装有处理器的无线通信终端的安全通信模式的方法，包括步骤：a) 基于从无线通信终端的语音编码器输出的语音数据中具有最低产生频率的数据而产生一个标记；b) 在发送终端，接收来自用户的对于安全通信的请求，并向接收终端发送该标记；和 c) 在该发送终端，基于从该接收终端发送的确认标记进入安全通信模式，并执行与该接收终端之间的安全通信。

附图说明

通过结合附图对给出的优选实施例的下列描述，本发明的上述和其他目的和特点将变得更加明显，其中：

图 1 是示出根据本发明实施例的无线通信系统的发送终端和接收终端的方框图；

图 2A 是示出根据本发明实施例的进入安全通信模式的发送终端的流程图；和

图 2B 是示出根据本发明实施例进入安全通信模式的接收终端的流程图。

具体实施方式

通过参考附图对下面给出的实施例的下列描述，本发明的其他目的和方

面将变得更加清楚。这里，对相同组件给出相同的附图标记，尽管他们出现在不同附图中。而且，如果对于相关现有技术的进一步详细描述被视为混淆本发明的观点，则将其省略。

图 1 是示出了根据本发明一个实施例的无线通信系统中发送终端和接收终端的方框图。如图中所示，该无线通信系统的发送终端包括麦克风 101、语音编码器 103、语音加密单元 105、信道编码单元 107 和扩频/调制单元 109。该接收终端包括扬声器 111、语音编码器 113、语音解密单元 115、信道解码单元 117 和解扩/解调单元 119。

输入至发送终端的麦克风 101 的用户的语音信号进入语音编码器 103，并以 20ms 时基（20ms-based）语音分组数据的形式输出。根据本发明，当发送终端，也就是主叫方，开始安全通信时，在语音加密单元 105 中产生用于安全通信的标记（token）。将该标记通过供发送该 20ms 时基语音分组数据之用的信道发送出去。简而言之，如果主叫方的用户尝试安全语音通信，则该语音加密单元 105 将该标记通过语音信道发送至接收终端，也就是被叫方。以这种方式，能实现安全语音通信。该标记的数据格式与该语音分组数据的数据格式相同。所以，无须附加设置该通信系统，即可进行安全语音通信。

同时，由于从语音编码器 103 输出的语音数据根据每一语音信号由随机数据组成，所以该标记数据应该能够区别于该语音分组数据。如果该标记数据不能区别于该语音分组数据，则接收终端不能分辨其从该发送终端所接收的信号是标记数据或语音分组数据。

为了使该标记数据区别于该语音分组数据，将具有最低产生频率的数据结合进从语音编码器 103 输出的语音数据中的任意长度，并将该数据用作该标记的首标。简而言之，在从语音编码器 103 输出的语音数据中，以例如两字节的预定长度形成的具有在例如三小时的预定时间的最低产生频率的数据被作为该标记的首标（称为“标记首标”）而存储在发送和接收终端中。从语音编码器 103 输出的语音分组数据的前两字节被存储预定时间，然后具有 0x0000~0xFFFF 的值中的最低频率的两字节数据被用作标记首标。

为了降低标记数据和语音分组数据重叠的可能性，可将具有从语音编码器 103 输出的具有多于 2 字节直到 22 字节的，例如在 8Kbps EVRC 语音编码器 103 的情况下，语音数据中最低产生频率的数据结合用作标记首标。

所希望的是, 该标记的长度必须短于语音编码器 103 的最大输出长度。如果该标记首标短于语音编码器 103 的最大输出数据, 则可将该标记的其他部分作为将在加密算法中使用的密钥值而发送。一般来说, 语音编码器 103 的输出数据具有各种长度, 例如全、半、1/4 和 1/8 速率。然而, 根据本发明, 希望在标记产生期间以全速率设置输出数据的长度。这是因为语音编码器 103 的最大输出长度可得到保障, 并且标记首标的长度可具有较宽选择范围。

语音编码器 103 的最大输出数据越长, 则该标记变得越长。所以, 可随该标记数据发送除了标记首标之外的信息。例如, 在数据加密标准异 (exclusive-OR) (DESX) 技术中, 使用主密钥和会话密钥以执行安全语音通信。对于发送和接收终端使用相同主密钥, 而会话密钥具有通过使用主密钥所产生的任意值。根据本发明, 如果发送终端产生的会话密钥被包括在标记中作为除了标记首标之外的信息, 则接收终端将从发送终端发送的会话密钥与接收终端中包含的使用主密钥而产生的会话密钥作比较 (以了解密钥是否匹配), 并判定是否进入安全通信模式。

接收终端的语音解密单元 115 判定从发送终端发送的数据是否为标记数据。这里, 发送终端的语音加密单元 105 重复发送相同标记数据预定次数 (例如, 重复发送 240 个 20ms 单位帧 4.8 秒), 并且如果接收终端重复接收被认为是包括如上所述标记首标的标记数据的相同数据预定次数 (例如, 接收 20ms 单位帧的相同数据 3 次), 可断定发送终端已尝试该安全语音通信。因此, 接收终端产生确认标记并向发送终端发送该确认标记。

以与发送终端的标记相同的方法产生和发送该确认标记。此时, 该确认标记首标与该标记首标相同或不同。发送该确认标记之后, 发送和接收终端进入安全通信模式并执行安全语音通信。这里, 判定密钥是否匹配的上述处理应理解为包括在判定发送终端是否正在尝试安全语音通信的处理之中。

图 2A 是示出了根据本发明一个实施例的进入安全通信模式的发送终端的流程图, 而图 2B 是示出了根据本发明一个实施例的进入安全通信模式的接收终端的流程图。

在步骤 S301, 发送终端处于正常通信模式。然后, 在步骤 S303, 判定用户是否输入尝试安全语音通信的请求。如果用户输入了尝试安全语音通信的请求, 在步骤 S305, 语音加密单元 105 基于预存储的标记首标产生标记

数据，并将其发送至接收终端，这也在上面描述过。

这里，语音加密单元 105 重复发送相同标记数据预定次数（例如，重复发送 240 个 20ms 单位帧 4.8 秒），并且如果接收终端重复接收相同数据预定次数（例如，接收 20ms 单位帧的相同数据 3 次），可认为发送终端已尝试安全语音通信。发送终端建立标记数据的临时长度，将其重复发送（例如，在重复发送 240 个 20ms 单位帧 4.8 秒的情况下）作为用于发送标记的标记发送时间。然后，在步骤 S307 和 S309，确定是否在标记发送时间内从接收终端发送确认标记，从标记数据发送的开始点建立该标记发送时间。

如果在标记发送时间期间没有接收到确认标记，则发送终端接着产生该标记数据并将它们发送至接收终端。当连续检验是否接收到确认标记时，如果标记发送时间超时，则逻辑进行到步骤 S301，并且发送终端保持正常通信模式。如果发送终端接收确认标记，因为确认标记的发送意味着接收终端已进入安全通信模式，则在步骤 S311，发送终端进入安全通信模式。

同时，在步骤 S313，接收终端保持为正常通信模式。然后，在步骤 S315，判定是否从发送终端发送了用于安全语音通信的标记数据。如果从发送终端发送了用于安全语音通信的标记数据，则在步骤 S317，语音解密单元 115 响应于用于安全语音通信的标记而产生确认标记，并向发送终端发送该确认标记。基于预存储的确认标记首标而产生确认标记数据，并将该确认标记数据发送至发送终端。

这里，在步骤 S319，语音解密单元 115 重复发送相同确认标记数据预定次数。在步骤 S307 和 S309，发送终端建立其在步骤 S305 重复发送的标记数据的临时长度，作为标记发送时间，例如在重复发送 240 个 20ms 单位的帧的情况下，该临时长度为 4.8 秒。然后，在步骤 S307 和 S309，判定是否在标记发送时间期间从接收终端发送确认标记，从标记数据发送的开始点建立该标记发送时间。如果接收到确认标记，则在步骤 S311，如前所述，发送终端进入安全通信模式。步骤 S319 之后，接收终端从正常通信模式进入安全通信模式。

本发明的方法可被实现为程序，并存储在例如 CD-ROM、RAM、ROM、软盘、硬盘、光-磁盘等的计算机可读记录介质中。

本发明的方法通过分析发送和接收终端的语音信号以及使用具有最低使用频率的数据作为标记数据而消除了发送用于进入安全通信模式的附加消息

或信号的需要。由于不需要附加消息，所以无须改变传统移动通信系统配置即可进行安全语音通信。

虽然已参照特定优选实施例描述了本发明，本领域普通技术人员应明白，在不脱离如所附权利要求定义的本发明的范围的情况下，可作出各种修改和变形。

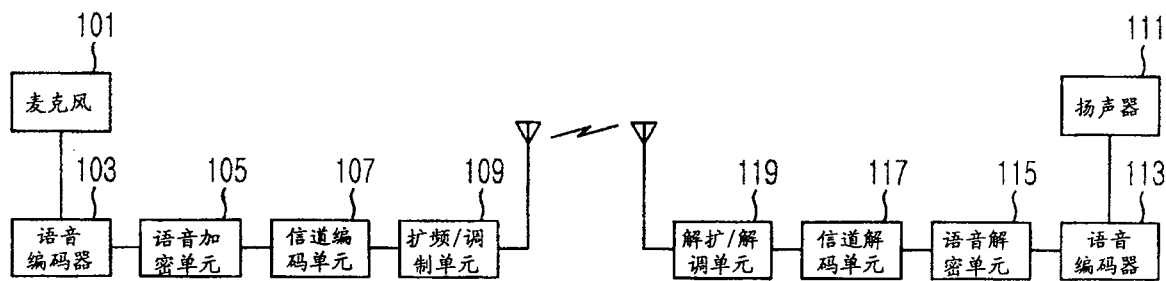


图 1

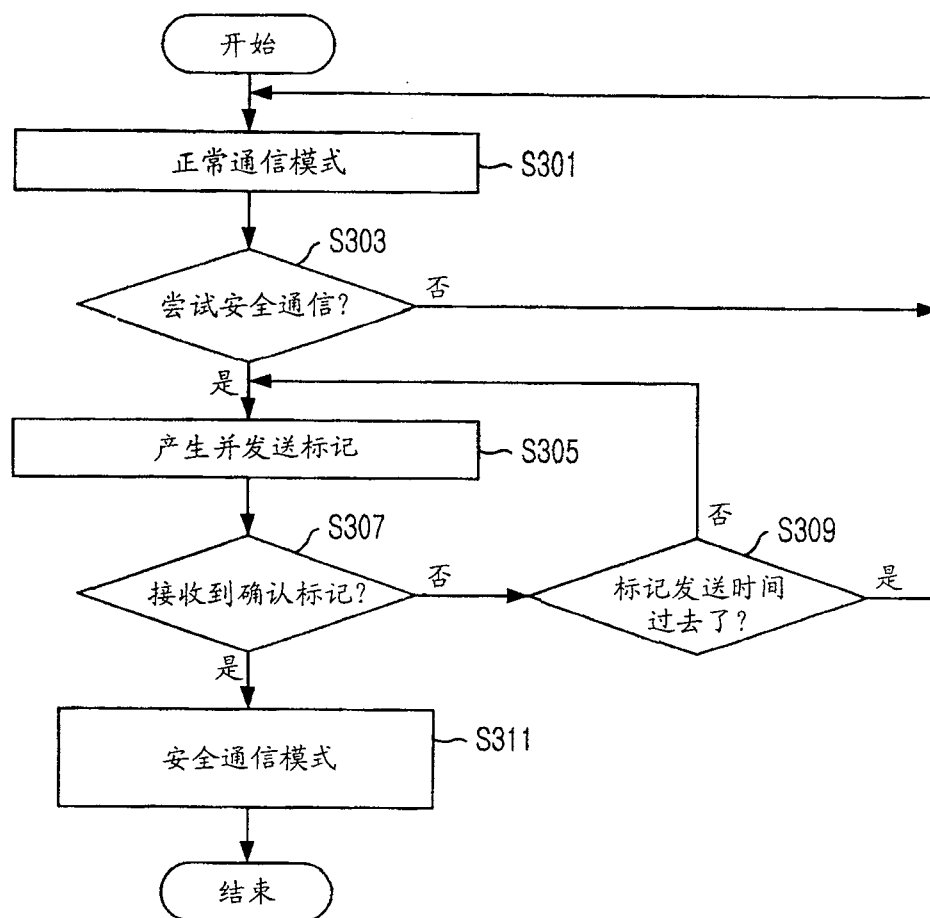


图 2A

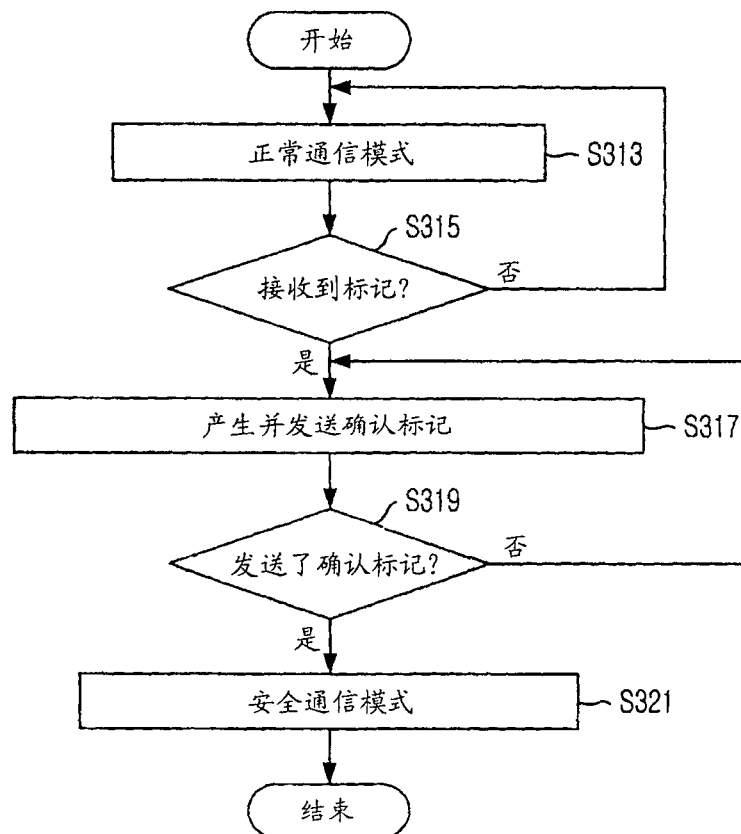


图 2B