

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200580032011.7

[51] Int. Cl.

H04K 1/02 (2006.01)

H04K 1/04 (2006.01)

[43] 公开日 2007 年 10 月 10 日

[11] 公开号 CN 101053191A

[22] 申请日 2005.9.12

[21] 申请号 200580032011.7

[30] 优先权

[32] 2004.9.23 [33] US [31] 10/947,724

[86] 国际申请 PCT/US2005/032540 2005.9.12

[87] 国际公布 WO2006/036532 英 2006.4.6

[85] 进入国家阶段日期 2007.3.22

[71] 申请人 摩托罗拉公司

地址 美国伊利诺伊州

[72] 发明人 迈克尔·克洛斯

[74] 专利代理机构 中原信达知识产权代理有限责任
公司

代理人 陆锦华 穆德骏

权利要求书 4 页 说明书 17 页 附图 6 页

[54] 发明名称

在无线通信系统中加密空中通信的方法和装置

[57] 摘要

为了改善在无线链路上发射的数据的加密，通信设备(202)在物理层处对码元进行加密。通信设备的码元映射器(208)接收包括多个比特的比特流，并且将多个比特映射到多个码元。通信设备的幅度和相位调节器(210)接收多个码元，并通过对每个码元施加相移和幅度调节的至少其中之一，对所述码元进行加密，以产生了用于经无线链路发射的多个加密码元。在本发明的另一实施例中，提供一种通信设备(250)，其能够通过对每个加密码元施加对应于由发射接收通信设备施加到码元的相移或幅度调节的相移和幅度调节中的至少其中之一，对加密码元进行解密。

1. 一种用于加密无线传输的方法，包括：
接收多个码元；
向所述多个码元中的每个码元施加相移和幅度调节的至少其中之一，以产生多个调节后的码元；以及
经由无线链路发射所述多个调节后的码元。
2. 如权利要求 1 的方法，其中，所述相移和幅度调节的至少其中之一是基于会话密钥和时隙编号的至少其中之一。
3. 如权利要求 1 的方法，进一步包括：生成码字，且其中向每个码元施加相移和幅度调节的至少其中之一包括：根据所述码字向所述多个码元中的每个码元施加相移和幅度调节的至少其中之一，以产生多个调节后的码元。
4. 如权利要求 1 的方法，其中，施加到所述多个码元的第一码元的相移和幅度调节的至少其中之一不同于施加到所述多个码元的第二码元的相移和幅度调节的至少其中之一。
5. 一种用于接收加密的无线传输的方法，包括：
经由无线链路接收多个加密码元，其中已经通过向所述多个加密码元中的每个码元施加相移和幅度调节中的至少其中之一，对所述码元进行了加密；以及
向所述多个加密码元中的每个加密码元施加相移和幅度调节的至少其中之一，以产生多个解密码元。
6. 如权利要求 5 的方法，其中，所述相移和幅度调节的至少其中之一是基于会话密钥和时隙编号的至少其中之一。

7. 如权利要求 5 的方法，进一步包括：生成码字，且其中向每个码元施加相移和幅度调节的至少其中之一包括：根据所述码字，向所述多个加密码元中的每个加密码元施加相移和幅度调节的至少其中之一，以产生多个解密码元。

8. 如权利要求 5 的方法，其中，施加到所述多个加密码元中的第一加密码元的相移和幅度调节的至少其中之一不同于施加到所述多个加密码元中的第二加密码元的相移和幅度调节的至少其中之一。

9. 一种通信设备，包括：

码元映射器，该码元映射器接收包括多个比特的比特流，以及将所述多个比特映射到多个码元；以及

幅度和相位调节器，该幅度和相位调节器从所述码元映射器接收多个码元，以及通过向所述多个码元中的每个码元施加相移和幅度调节中的至少其中之一，对每个码元进行加密，以产生用于经无线链路传输的多个调节后的码元。

10. 如权利要求 9 的通信设备，其中，所述码元映射器包括第一码元映射器，且其中所述通信设备进一步包括：

第二码元映射器，该第二码元映射器接收所述多个调节后的码元，以及将所述多个调节后的码元中的每个调节后的码元映射到时隙中的码元位置；

调制器，该调制器对所述时隙中的所述码元进行调制，以产生调制的时隙；以及

功率放大器，该功率放大器对所述调制的时隙进行放大，以产生用于经无线链路传输的放大时隙。

11. 如权利要求 9 的通信设备，其中，所述通信设备进一步包括：至少一个存储器设备，该存储器设备保存会话密钥和时隙编号中的至少其中之一，以及其中相移和幅度调节中的所述至少其中之一是基于

会话密钥和时隙编号中的所述至少其中之一。

12. 如权利要求 9 的通信设备, 其中, 所述通信设备进一步包括: 耦合到所述幅度和相位调节器的码字生成器, 所述码字生成器生成码字, 且其中所述幅度和相位调节器根据所述码字, 通过向所述多个码元中的每个码元施加相移和幅度调节的至少其中之一, 向所述码元施加相移和幅度调节的至少其中之一。

13. 一种通信设备, 包括:

幅度和相位调节器, 该幅度和相位调节器接收已经在无线链路发射上的多个加密码元, 其中已经通过向所述多个加密码元中的每个码元施加相移和幅度调节中的至少其中之一, 对所述码元进行了加密, 以及向所述多个加密码元中的每个加密码元施加相移和幅度调节中的至少其中之一, 以产生多个解密码元; 以及

反向码元映射器, 该反向码元映射器接收多个解密码元, 并将所述多个解密码元中的每个解密码元映射到星座中的点, 以产生比特流。

14. 如权利要求 13 的通信设备, 其中, 所述码元映射器包括第一码元映射器, 以及其中所述通信设备进一步包括:

解调器, 该解调器接收已经经无线链路发射的时隙, 以及对所述时隙进行解调, 以产生解调时隙; 以及

第二码元映射器, 该第二码元映射器接收所述解调时隙, 并且对所述时隙进行解交织, 以产生所述多个加密码元。

15. 如权利要求 13 的通信设备, 其中, 所述通信设备进一步包括: 至少一个存储器设备, 该存储器设备保存会话密钥和时隙编号中的至少其中之一, 以及其中相移和幅度调节中的所述至少其中之一是基于会话密钥和时隙编号中的所述至少其中之一。

16. 如权利要求 13 的通信设备, 其中所述通信设备进一步包括:

耦合到所述幅度和相位调节器的码字生成器，所述码字生成器生成码字，且其中所述幅度和相位调节器根据所述码字，通过向所述多个码元中的每个码元施加相移和幅度调节的至少其中之一，向所述码元施加相移和幅度调节的至少其中之一。

在无线通信系统中加密空中通信的方法和装置

相关联申请的交叉引用

本申请与美国专利申请序号_____相关联，其与本申请同日提交，代理号为 No.CE13323R。

技术领域

本发明总的来说涉及无线通信系统，且更具体地涉及在无线通信系统中对空中通信进行加密。

背景技术

在通常的无线通信系统中，当建立通信会话时，在发射和接收通信设备之间指配会话密钥。随后，通过发射通信以执行通过空中发射的数据的层 2 或层 3 的加密，使用该会话密钥。不执行物理层（即，层 1）加密，也就是说，没有对调制波形进行加密。此外，通常仅仅加密用户数据而不对导频码元和同步码元进行加密，其中该码元必须被用作定时同步和衰落恢复的参考。

层 2 或层 3 加密的性能使得数据容易受到截听通信设备进行的解密的攻击，所述截听通信设备截听会话密钥或者通过强力应用程序来解密数据。因此，需要存在一种方法和装置，使得空中接口相对于无线通信系统中通信的不期望的截听者来说更加安全。

附图说明

图 1 示出了根据本发明实施例的无线通信系统的框图。

图 2 示出了根据本发明实施例的图 1 的无线通信系统的结构框图。

图 3 示出了根据本发明实施例的图 2 的发射通信设备的操作的逻辑流程图。

图 4 示出了根据本发明实施例的图 2 的发射通信设备的幅度和相位调节器的操作的图示。

图 5 示出了根据本发明实施例的图 2 的接收通信设备的操作的逻辑流程图。

图 6 示出了根据本发明另一实施例的发射通信设备的信号处理单元的框图。

图 7 示出了根据本发明另一实施例的示例性时隙的框图。

图 8 示出了根据本发明另一实施例的接收通信设备的信号处理单元的框图。

具体实施方式

为了解决对于如下装置和方法的需要，其中所述装置和方法使得空中接口相对于无线通信系统中通信的不期望的截听者所进行的解密来说更加安全，提供一种通信设备，其在物理层处对码元进行加密，以改善在无线链路上发射的数据的加密。通信设备的码元映射器接收包括多个比特的比特流，并且将多个比特映射到多个码元。通信设备的幅度和相位调节器接收多个码元，并通过对多个码元中的每个码元施加相移和幅度调节的至少其中之一，对所述码元进行加密，以产生了用于在无线链路上传输的多个加密码元。在本发明的另一实施例中，提供一种通信设备，其能够通过对每个加密码元施加相移和幅度调节中的至少其中之一，对加密码元进行解密，其中所述每个加密码元对应于由发射通信设备施加到码元的相移或幅度调节。

通常本发明的实施例包括一种用于加密无线传输的方法。该方法包括：接收多个码元；对多个码元中的每个码元施加相移和幅度调节的至少其中之一，以产生多个调节后的码元；以及经由无线链路发射该多个调节后的码元。

本发明的另一实施例包括一种用于接收加密无线传输的方法。该方法包括：经由无线链路接收多个加密码元，其中已经通过向所述码

元施加相移和幅度调节的至少其中之一，对多个加密码元的每个码元进行了加密；以及向多个加密码元中的每个加密码元施加相移和幅度调节的至少其中之一以，产生多个解密码元。

本发明的又一实施例包括一种通信设备，其包括：码元映射器，该码元映射器接收包括多个比特的比特流，并且将多个比特映射到多个码元。该通信设备进一步包括：幅度和相位调节器，其从码元映射器接收多个码元，并向多个码元中的每个码元施加相移和幅度调节的至少其中之一，以产生用于经无线链路传输的多个调节后的码元。

本发明的又一实施例包括一种通信设备，其包括：幅度和相位调节器，该幅度和相位调节器接收已经经无线链路发射的多个加密码元，其中已经通过向多个加密码元的每个码元施加相移和幅度调节的至少其中之一，对所述码元进行了加密，以及向多个加密码元中的每个加密码元施加相移和幅度调节的至少其中之一，以产生多个解密码元。该通信设备进一步包括：反向码元映射器，其接收多个解密码元并将多个解密码元的每个解密码元映射到星座中的点，以产生比特流。

可以参考图 1-8 更加充分地描述本发明。图 1 示出了根据本发明实施例的无线通信系统 100 的框图。通信系统 100 包括：基站收发信机站（BTS）102，其能够经由空中接口 104 参与同移动站（MS）110 的无线通信，所述移动站例如是蜂窝电话、无线电电话、或无线数据调制解调器。空中接口 104 包括前向链路 108，该前向链路 108 包括业务信道、导频信道、寻呼信道和信令信道。空中接口 104 进一步包括反向链路 106，该包括反向链路 106 业务信道、接入信道和信令信道。

图 2 示出了根据本发明实施例 100 的通信系统的体系结构的框图。在通信系统 100 的发射侧，诸如 BTS102 的发射通信设备 202 接收比特流，将比特流转换为相应的码元流，通过对码元流进行加密从而在物理层处提供加密，以产生加密码元流，并且经由诸如空中接口 104 的

空中接口发射所述加密码元流。在通信系统 100 的接收侧, 诸如 MS110 的接收通信设备 250 接收所发射的加密码元流, 并通过对接收码元进行解密, 从而提供物理层处的解密, 以恢复与每个接接收到的数据码元相对应的发射比特流的比特。然而, 本领域普通技术人员可以意识到, 相对于本发明的实施例而言, 每个 BTS102 和 MS110 都可以被操作作为发射通信设备或者接收通信设备。

每个发射通信设备 202 和接收通信设备 250 包括各自的信号处理单元 204、270, 例如是本领域普通技术人员所公知的一个或多个微处理器、微控制器、数字信号处理器 (DSP)、或上述其他设备的组合。如本领域普通技术人员所意识到的, 此处描述的信号处理单元 204、270 的各种功能可以可替换地以硬件电路实现, 例如可编程逻辑阵列 (PLA) 或专用集成电路 (ASIC)。信号处理单元 204 包括前向纠错 (FEC) 编码器 206、耦合到该编码器的码元映射器 208、耦合到所述码元映射器的幅度和相位调节器 210、以及耦合到该幅度和相位调节器的码字生成器 212。信号处理单元 270 包括: 幅度和相位调节器 272、每个都耦合到幅度和相位调节器的导频内插功能 274 以及码字生成器 280、耦合到导频内插功能的反向码元映射器 276、以及耦合到反向码元映射器的 FEC 解码器 278。

每个发射通信设备 202 和接收通信设备 250 进一步包括各自的与各自的信号处理单元相关联的至少一个存储器设备 230、290, 例如随机存取存储器 (RAM)、动态随机存取存储器 (DRAM)、和/或只读存储器 (ROM) 或其等效物, 所述存储器设备保存可以由信号处理单元执行且允许信号处理单元操作通信系统 100 的数据和程序。每个发射通信设备 202 和接收通信设备 250 进一步在其各自的至少一个存储器设备 230、290 中保存会话密钥, 如在现有技术中已知的, 在发射和接收通信设备之间建立通信会话期间, 通过这两个通信设备交换该会话密钥。每个发射通信设备 202 和接收通信设备 250 可以进一步在其各自的至少一个存储器设备 240、290 中保存唯一地与 MS110 相关联的

移动序号。当通信系统 100 是时分多址通信系统时，每个发射通信设备 202 和接收通信设备 250 可以进一步在其各自的至少一个存储器设备 230、290 中保存时隙编号，如在现有技术中已知的，在建立通信会话期间，该时隙编号被指配给 MS110。

图 3 示出了根据本发明实施例 100 的发射通信设备 202 的操作的逻辑流程图 300。现在参考图 2 和 3，当数据源（未示出）向信号处理单元 204 提供数据流，优选地以例如比特的二进制格式提供时，逻辑流程图 300 开始（302），其中所述数据流实际上可以包括任何能够以数字格式表示的数据，包括但不限于，语音和图像数据。信号处理单元 204 将该数据路由到编码器 206。编码器 206 对该数据应用纠错码，优选地应用前向纠错码（FEC）。例如，编码器 206 可以通过利用例如 Viterbi 编码算法的卷积码对数据进行编码，然而也可以使用分组码（block code）。卷积码和分组码在现有技术中都是公知的，且不对其进行更详细的描述。所使用的纠错码的类型并非本发明的关键，且本领域普通技术人员可以意识到在不背离本发明的精神和范围的情况下可以对数据应用多种类型的纠错码。无论如何，编码器 206 的输出包括优选地以二进制数据（比特）格式表示的信息。

编码器 206 输出的数据流随后被提供至码元映射器 208。然而，在本发明的另一实施例中，数据源提供的数据流可以被直接进入到码元映射器 208。在本发明的又一实施例中，信号处理单元 204 可以进一步包括交织器，其在编码器 206 将编码数据传送至码元映射器 208 之前对编码数据进行交织。

码元映射器 208 将编码数据映射（306）到被包括在码元星座（constellation）中的多个码元中的一个，以产生了包含有与该编码数据相对应的多个码元的码元流。优选地，码元映射器 208 利用正交幅度调制（QAM）映射方案对数据进行映射。然而，所使用的映射方案对于本发明而言不是关键点，且本领域普通技术人员知道多种映射方

案，在不背离本发明的精神和范围的情况下，在这里可以使用诸如二进制相移键控（BPSK）或正交相移键控（QPSK）。

为了映射数据流，码元映射器 208 将输入数据流分为 P 二进制数据单元（例如数据比特）的组，以形成多个 P 元组。随后，通过将该 P 元组映射到预定 QAM 星座中的 M 个可能的点中的对应点，码元映射器 208 对多个 P 元组中的每一个进行调制，其中， $M=2^P$ 。为此，预定的 QAM 星座包括在多维空间内定义的 M 个可能的点，优选地在复数的二维（I/Q）空间。在该二维空间内的每个点可以认为是二进制基本向量的向量和。二进制基本向量分别相应于星座点的同相（I）分量和正交（Q）分量，或相应的数据码元。用于定义特定点的两个基向量的各自的幅度可以被认为是该点的二维坐标（I,Q）。然而，本领域普通技术人员可以认识到，星座中的每个点可以可替换地由相应的幅度和相位来表示。在通过码元映射器 208 调制每个 P 元组之后，码元映射器将所获得的码元传送至幅度和相位调节器 210。

随后，通过对幅度和相位调节器接收到的每个码元施加相移“ θ ”和幅度调节“A”的至少其中之一，幅度和相位调节器 210 对该码元进行加密（308），以产生加密的、相位和/或幅度调节过的码元。优选地，相位和/或幅度调节基于会话密钥，其中所述会话密钥是由发射通信设备 202 和接收通信设备 250 在通信会话建立期间交换的、且保存在其各自的至少一个存储器设备 230、290 中。当通信系统 100 是时分多址（TDMA）通信系统时，相位和/或幅度调节可以进一步基于指配给 MS110 的时隙编号。

更具体地，由幅度和相位调节器 210 施加的每个相移“ θ ”和幅度调节“A”是基于由码字生成器 212 生成的码字。在本发明的一个实施例中，码字生成器 212 包括由信号处理单元 204 执行的加密算法，例如在 3GPP（第三代合作伙伴计划）TS（技术规范）55.21 6v6.2.0 中描述的先进加密标准（Advanced Encryption Standard）（AES）算法、

或 A5/3 或 GEA3 加密算法, 该技术规范因此通过引用被完全包括于此。该算法的输入包括: 会话密钥或会话的衍生物, 以及可以进一步包括时隙编号或时隙编号的衍生物, 例如时隙编号的散列版本 (hashed version)。随后, 从加密算法的对应输出获得相移 “ θ ” 和幅度调节 “A”。例如, 幅度和相位调节器 210 施加于码元的相移 “ θ ” 和幅度调节 “A” 可以基于加密算法所输出的最初的 “n” 比特, 或者相移 “ θ ” 可以基于加密算法所输出的最初的 “n” 比特且幅度调节 “A” 可以基于该算法所输出的接下来的 “m” 比特。

例如, 假定 “n” =4。与幅度和相位调节器 210 的码元输入相对应地, 幅度和相位调节器读取由码字生成器 212 输出的 4 比特。通过一次读取 4 比特, 通信系统 100 可以实现 “ $360^\circ / 2^n$ ” 或者 22.5° 的相移增量。随后, 幅度和相位调节器 210 施加的相移 “ θ ” 可以是 “ $N \times (360^\circ / 2^n)$ ”, 其中 “N” 是对应于 “n” 比特的值。例如, 假定信号处理单元 204 读出的 ‘n’ 比特是 ‘1001’。这些比特对应于值 ‘9’ 即, $N=9$ 。结果, 由幅度和相位调节器 210 施加的对应的相移 ‘ θ ’ 可以是 ‘ 9×22.5 ’, 或者 202.5° 。结果, 如果输入到幅度和相位调节器 210 的码元具有 45° 的相位 ‘ φ ’, 则幅度和相位调节器 210 输出的对应的相移码元具有 ‘ $\varphi + \theta$ ’ 的相位, 也就是, 247.5° 。类似地, 当 ‘n’ (或者 ‘m’) =4 时, 该 ‘n’ (或者 ‘m’) 比特可以用于确定码元的幅度调节。例如, 当所述比特对应于值 ‘9’ 时, 该值可以用于确定幅度变化的分数或者百分比。本领域技术人员可以想到很多种根据码字生成器 212 输出的码字调节码元的相位或幅度的算法, 且在不背离本发明的精神和范围的情况下可以在这里使用上述的任何算法。

对于输入到幅度和相位调节器 210 的每个相继的码元来说, 幅度和相位调节器在任何适当的位置读取由码字生成器 212 输出的接下来的相继 ‘n’ 比特或 ‘n+m’ 比特。为了实现该相位且幅度调节, 幅度和相位调节器 210 可以包括缓冲器, 其存储码字生成器 212 的码字, 且根据该码字, 幅度和相位调节器可以读取 ‘n’ 或 ‘n+m’ 比特。

当在发射通信设备 202 和接收通信设备 250 之间建立通信会话时，信号处理单元 204 通过将会话密钥输入到码字生成器 212 中，使码字生成器 212 初始化，所述会话密钥通常是比特串或者从会话密钥获得的比特串，和/或时隙编号、或者从时隙编号获得的比特串，诸如时隙编号的散列版本。与每个输入到幅度和相位调节器 210 中的码元相对应，幅度和相位调节器 210 读取码字生成器 212 的输出的‘n’或者‘n+m’比特。‘n’和‘m’的值被保存在发射和接收通信设备 202、250 的每一个的至少一个存储器设备 230、290 中。随后，信号处理单元 204 根据所读取的‘n’比特确定相移‘ θ ’或者幅度调节‘A’，或者根据该‘n’比特确定相移‘ θ ’以及根据码字接下来的‘m’比特确定幅度调节‘A’。

在本发明的另一实施例中，码字生成器 212 可以包括诸如线性反馈移位寄存器（LFSR）的移位寄存器，其保持于信号处理单元 204 中或至少一个存储器设备 230 中。当在发射通信设备 202 和接收通信设备 250 之间建立通信会话时，信号处理单元 204 将会话密钥或者从该会话密钥获得的比特串写入移位寄存器，并且可以进一步将时隙编号或者从该时隙编号获得的比特串写入移位寄存器。与输入到幅度和相位调节器 210 的每个码元相对应，信号处理单元 204 随后读取移位寄存器的‘n’或者‘n+m’比特，优选地是移位寄存器 212 中的最低有效的‘n’或者‘n+m’比特。信号处理单元 204 每次从移位寄存器 212 读取‘n’或者‘n+m’比特，信号处理单元就随后在读出与下个相位和/或幅度调节相对应的值之前，在移位寄存器中移动一个或多个比特，并且写入一个或多个新的最高有效比特。移位寄存器算法可以被保存在发射和接收通信设备 202、250 中的每一个的至少一个存储器设备 230、290 中，所述移位寄存器算法与移位寄存器的移位相对应，即，与每次相位和/或幅度调节被读出时移位寄存器移位的比特的数目相对应，以及与如何确定新的一个或多个最高有效比特相对应。已知多种上述算法，并且此处使用的特定的算法对于本发明来说并非关键性的。

为了帮助读者理解本发明，并且仅仅为了示出本发明的原理而非意图以任何方式限制本发明，通过图 4 示出了幅度和相位调节器 210 施加的相移的图解说明。输入到幅度和相位调节器 210 中的码元 (I,Q) 被显示为具有幅度|R|以及相位 φ 。移位寄存器 212 输出与相移 ' θ ' 相对应的码字，以及将该码字输入到幅度和相位调节器 210。随后，幅度和相位调节器 210 输出相移码元 (I',Q')，该相移码元具有幅度|R|以及相位 ' $\varphi + \theta$ '。

如在现有技术中已知的，在被称为帧的组中空中发射数据。在建立通信会话之后，每次发射通信设备 202 开始新的帧时，信号处理单元 204 都是码字生成器 212 重新初始化，从而使得及时地根据重新初始化过的码字生成器而对被加密用于嵌入在新帧中的第一码元进行加密。新帧的报头包括新帧指示符 (NFI)，其指出这是新的帧，以及该 NFI 向接收通信设备 250 指出接收通信设备应该同时是其码字生成器重新初始化。由此，在发射和接收通信设备 202、250 的各自的码字生成器 212、280 之间保存同步。

幅度和相位调节器 210 将每个相位和/或幅度调节后的码元传送到耦合到信号处理单元 204 的发射通信设备 202 的发射机部分 220。发射机部分 220 包括耦合到放大器 224 的调制器 222。发射机部分 220 将相位和/或幅度调节后的码元路由至调制器 222。调制器 222 将每个加密过的、相位和/或幅度调节后的码元调制 (310) 到射频 (RF) 载波上，以产生调制载波并将调制载波传送到放大器 224。放大器 224 放大 (312) 所述调制载波，以产生放大信号，并随后经由天线 226 和空中接口 104 发射 (314) 该放大信号。随后，逻辑流程 300 结束 (316)。

现在参考图 5、示出了根据本发明实施例的通信系统 100 的接收通信设备 250 的操作的逻辑流程图 500。接收通信设备 250 执行了相对于发射通信设备 202 相反的功能。当接收通信设备 250 的天线 252 接

收到发射通信设备 202 发射的调制载波并将接收到的调制载波路由至接收通信设备的接收机部分 260 时, 逻辑流程 500 开始 (502)。接收机部分 260 包括解调器 264, 并可以进一步包括耦合到解调器的低噪声放大器 (LNA) 262。当接收机部分 260 接收到调制载波时, 接收机部分将接收信号路由至 LNA262, 其对调制载波进行放大并将放大的接收信号路由至解调器 264。解调器 264 通过移除载波来解调 (504) 该放大信号, 以产生包括多个加密码元的基带的、加密的码元流。随后, 解调器 264 将基带、加密的码元流路由至接收通信设备 250 的信号处理单元 270。

信号处理单元 270 将基带、加密的码元流路由至幅度和相位调节器 272。幅度和相位调节器 272 通过向加密码元施加这样的相位和/或幅度调节, 对每个加密码元进行解密 (506), 所述相位和/或幅度调节对通过幅度和相位调节器 210 添加给码元的相位和/或幅度调节进行了补偿, 由此产生了多个解密码元。例如, 在本发明的一个实施例中, 幅度和相位调节器 272 可以从码元的相位减去下述相移, 即, 该相移与幅度和相位调节器 210 施加到码元的相移相等。在本发明的另一实施例中, 幅度和相位调节器 272 可以向码元的相位添加下述相移, 即, 该相移将完成码元围绕复平面的 360° 旋转, 即, 可以施加近似等于 ' $360^\circ - \theta$ ' 的相移。例如, 如果幅度和相位调节器 210 向码元施加 202.5° 的相移, 则幅度和相位调节器 272 可向该码元施加约 ' $360^\circ - 202.5^\circ$ ' 或者 157.5° 的相移。类似地, 幅度和相位调节器 272 向加密码元施加幅度调节, 该幅度调节与幅度和相位调节器 210 施加的幅度调节相反。

幅度和相位调节器 272 实现的相位和/或幅度调节基于与如下所述的码字相同的码字, 其中所述码字是用于确定幅度和相位调节器 210 中的对应相位和/或幅度调节的码字。耦合到幅度和相位调节器 272 的码字生成器 280 生成该码字。码字生成器 280 与码字生成器 212 相类似地操作, 并且根据会话密钥产生该码字, 以及可以进一步根据

时隙编号产生码字，其中会话密钥和时隙编号被保存在接收通信设备 250 的至少一个存储器设备 290 中。

当首先在发射通信设备 202 和接收通信设备 250 之间建立通信会话时，信号处理单元 270 通过将会话密钥或从该会话密钥获得的比特串输入到码字生成器中，使码字生成器 280 初始化，并且可以进一步将时隙编号或者从该时隙编号获得的比特串输入到码字生成器中。随后，对于输入到幅度和相位调节器 210 中的每个码元，幅度和相位调节器随后读取码字生成器 280 产生的‘n’或‘n+m’比特的码字，该‘n’和‘m’值被保存在接收通信设备 250 的至少一个存储器设备 290 中。随后，幅度和相位调节器 272 根据该‘n’或‘n+m’比特确定相移和/或幅度调节，且将所确定的相移和/或幅度调节施加到该码元，以产生解密码元。在建立通信会话之后，每次接收通信设备 250 接收到新的帧时，信号处理单元 270 都使码字生成器 280 重新初始化，从而使得及时地根据重新初始化过的码字生成器，对自该新的帧解密的第一码元进行解密。

与幅度和相位调节器 210 相类似地，幅度和相位调节器 272 可以包括缓冲器，其存储码字生成器 280 输出的码字，且幅度和相位调节器可以从该码字读取‘n’或‘n+m’比特。

随后，幅度和相位调节器 272 将多个解密码元路由至导频内插功能 274。为了减轻衰落效果，导频内插功能 274 根据所接收到的先验（apriori）信号在多个解密码元上执行导频内插，如在现有技术中已知的，所述先验信号例如是导频信号和同步信号。随后，导频内插功能 274 将衰落校正的多个解密码元路由至反向码元映射器 276。反向码元映射器 276 与码元映射器 208 相对应，并且执行与码元映射器 208 相反的功能。根据码元映射器 208 使用的码元映射方案，通过恢复与每个码元相对应的 P 元组，反向码元映射器 276 产生 (510) 恢复比特流。随后，反向码元映射器 276 将恢复比特流传送到解码器 278，优选地，

其为 FEC 解码器。解码器 278 根据编码器 206 所使用的编码算法对恢复比特流进行解码 (512)，以产生解码比特流。随后，根据公知的信号处理技术，接收通信设备 250 对该解码比特流进行进一步处理 (514)，且逻辑流程 500 结束 (516)。在本发明的其他实施例中，取决于发射通信设备 202 的特征，接收通信设备 250 可能不包括解码器或者可能进一步包括解交织器。

通过向将被经由无线链路发射的多个码元中的每个码元施加相移和幅度调节中的至少其中之一，发射通信设备 202 提供了物理层加密，其改进了现有技术的在无线链路上发射数据的加密。向现有技术的层 2 或层 3 加密添加物理层加密，使得数据相对于通过截听通信设备进行解密而言更加安全，其中所述通信设备或者截听会话密钥或者通过强力应用程序来尝试对数据进行解密。

在本发明的另一实施例中，时分多址 (TDMA) 实施例，发射通信设备的信号处理单元可以进一步包括如下组件，所述组件用于单独地处理和与时隙中插入各种数据类型，所述数据类型例如是导频数据、同步数据和用户数据。现在参考图 6，示出了根据本发明的 TDMA 实施例的发射通信设备的信号处理单元 600 的框图。信号处理单元 600 为多种数据类型提供了并行处理，所述的数据类型例如是导频数据、同步数据和用户数据。为了提供并行处理，信号处理单元 600 包括用于处理多种数据类型的多个码元映射器、和多个幅度和相位调节器。

编码器 604，优选地 FEC 编码器，接收与用户数据相关联的比特流。编码器 604 与编码器 206 相类似地操作，且如上关于编码器 206 所述地，对编码器接收到的数据进行编码，以产生编码数据。对于本发明来说，编码器的类型既不是关键的，也并不是一定需要的特定的编码。

编码器 604 将编码器产生的编码数据传送到多个码元映射器

606-608 中的一个（示出了三个），例如码元映射器 608。例如导频数据和同步数据的其他数据类型被直接传送到多个码元映射器 606-608 的其他码元映射器，例如码元映射器 604 和 606。每个码元映射器 606-608 与码元映射器 208 相类似地操作，并且将码元映射器接收到的数据映射到被包括在码元星座中的多个码元中的一个，以产生了对应于该编码数据的码元流。在本发明的另一实施例中，进入编码器 604 的数据流可以被直接输入到码元映射器 608，而不用通过编码器 604。在本发明的又一实施例中，信号处理单元 204 可进一步包括多个交织器，其每一个在编码器将编码数据传送至对应的码元映射器之前对编码数据进行交织。

随后，每一码元映射器 606-608 将码元映射器产生的码元流传送到幅度和相位调节器单元 610。幅度和相位调节器单元 610 包括多个幅度和相位调节器 610₁-610₃（示出了三个），且幅度和相位调节器是为每个对应的数据类型和关联的码元映射器 606-608 分配的。幅度和相位调节器单元 610 耦合到码字生成器 612，且多个幅度和相位调节器 610₁-610₃ 的每一幅度和相位调节器根据码字生成器输出的码字，向幅度和相位调节器接收到的每一码元施加相移，以产生加密的、相移的码元。

优选地，每个幅度和相位调节器 610₁-610₃ 与幅度和相位调节器 210 相类似地操作，且码字生成器 612 与码字生成器 212 相类似地操作。信号处理单元 600（且更加具体地，幅度和相位调节器单元 610）将码字生成器 612 输出的码字的最初‘n’比特，即‘n₁’比特或者最初‘n+m’比特，即“(n+m)₁”比特提供给多个幅度和相位调节器的第一幅度和相位调节器，例如是幅度和相位调节器 610₁。幅度和相位调节器单元 610 将码字生成器 612 输出的码字的第二不同的‘n’比特，即‘n₂’比特或者第二不同的‘n+m’比特，即“(n+m)₂”比特提供给多个幅度和相位调节器的第二幅度和相位调节器，例如是幅度和相位调节器 610₂。幅度和相位调节器单元 610 将码字生成器 612 输出的码字的

第三不同的‘n’比特，即‘ n_3 ’比特或者第三不同的‘n+m’比特，即“(n+m)₃”比特提供给多个幅度和相位调节器的第三幅度和相位调节器，例如是幅度和相位调节器 610₃。对于接下来输入到相同幅度和相位调节器 610₁-610₃ 的每个码元，码字生成器 612 输出的码字的另一不同的‘n’或者‘n+m’比特被提供至该幅度和相位调节器。然而，在本发明的另一实施例中，诸如幅度和相位调节器 610₂ 的根据同步码元操作的幅度和相位调节器可以向所有同步码元施加相同的相移，以便使得与接收通信设备中的同步码元相关联的自相关值最大化。幅度和相位调节器单元 610 可以进一步包括缓冲器，其存储码字生成器 612 输出的码字，且根据该码字，幅度和相位调节器单元可以读取被提供至每个幅度和相位调节器 610₁-610₃ 的‘n’或者‘n+m’比特。

随后，每个幅度和相位调节器 610₁-610₃ 将幅度和相位调节器产生的每个相位和/或幅度调节后的码元传送到时隙码元映射器 614。时隙码元映射器 614 将从幅度和相位调节器 610₁-610₃ 接收到的每个相位和/或幅度调节后的码元映射到时隙中适当的块。例如，图 7 示出了可以在本发明 TDMA 实施例中使用的示例性时隙 700 的框图。在时隙期间，时隙的指配用户有权使用相关联射频（RF）信号的全部频谱。如图 7 所示，时隙 700 包括四个频率子信道 701-704，即，四个信号路径，其每一个与单独的偏移频率处的信号混频，以产生指定 RF 频谱的频率子信道。由于混频信号的频率偏移，因此每一子信道 701-704 偏离于其他子信道。例如，时隙 700 可以是可从 Illinois, Schaumburg 的 Motorola, Inc. 获得的“iDEN”无线系统设备使用的“iDEN”时隙。时隙 700 中的每个子信道 701-704 可以包括整个时隙 700 中总共 212 个码元位置中的 53 个码元位置。时隙码元映射器 614 可以随后对每个子信道 701-704 的最初三个码元位置中的三个同步码元（该码元位置在时隙 700 中由‘S’表示）进行交织，并且进一步在每个子信道 701-704 中的预定码元位置（该码元位置在时隙 700 中分别由‘P’和‘D’表示）中利用用户数据码元对导频码元进行交织。

随后，时隙码元映射器 614 将该时隙路由至发射机部分，在那里时隙被调制到射频（RF）子信道上，且调制信号被放大，以产生被发射到接收通信设备的放大 RF 信号。

类似地，在 TDMA 实施例中，接收通信设备的信号处理单元可以对应地包括如下组件，所述组件用于单独地处理由对应的发射通信设备发射的各种数据类型，所述数据类型例如是导频数据、同步数据和用户数据。现在参考图 8，示出了根据本发明的 TDMA 实施例的接收通信设备的信号处理单元 800 的框图。信号处理单元 800 执行与信号处理单元 600 相反的功能。更具体地，信号处理单元 800 包括反向时隙码元映射器 802，其对已经被接收通信设备的接收机部分的解调器下变频为基带的时隙进行接收，并且对被设置在时隙的码元位置中的码元进行解交织。随后，反向时隙码元映射器 802 将每个码元路由至幅度和相位调节器单元 804。

幅度和相位调节器单元 804 包括多个幅度和相位调节器 804_1 - 804_3 （示出了三个），且幅度和相位调节器被指配用于每个对应的数据类型（例如导频数据、同步数据和用户数据）和相关联的反向码元映射器 812-814。幅度和相位调节器单元 804 耦合到码字生成器 806，该码字生成器与码字生成器 280 相类似地操作且将一个或多个编码字发送（source）至幅度和相位调节器单元 804。随后，根据由码字生成器 806 发送的一个或多个编码字，每个幅度和相位调节器 804_1 - 804_3 通过向码元施加相移和/或幅度调节，对幅度和相位调节器接收到的每个码元进行解密，以产生解密码元。优选地，每个幅度和相位调节器 804_1 - 804_3 与幅度和相位调节器 272 相类似地操作。此外，对于幅度和相位调节器接收到的每个不同的码元来说，在幅度和相位调节器单元将不同的‘n’或者‘n+m’比特提供至每个不同的幅度和相位调节器 804_1 - 804_3 且进一步提供至每个相同的幅度和相位调节器方面，幅度和相位调节器单元 804 的操作与幅度和相位调节器单元 610 相类似。然而，在本发明的另一种实施例中，取决于发射通信设备中对应的幅度和相位调

节器施加到同步码元的相移，诸如幅度和相位调节器 804₂ 的、对同步码元进行操作的幅度和相位调节器可以向所有同步码元施加相同的相移。幅度和相位调节器单元 804 可以进一步包括缓冲器，其存储码字生成器 806 输出的码字，且根据码字，幅度和相位调节器单元可以读取被提供至每个幅度和相位调节器 804₁-804₃ 的 ‘n’ 或者 ‘n+m’ 比特。

随后，每个幅度和相位调节器 804₁-804₃ 将幅度和相位调节器产生的每个调节后的码元路由到导频内插功能 810。与导频内插功能 274 相类似，导频内插功能 810 根据接收到的先验数据，对导频内插功能接收到的每个调节过的用户数据码元进行导频内插，如在现有技术中已知的，所述先验数据例如是导频数据以及同步数据。导频内插功能 810 可以随后丢弃 (drop) 接收到的导频数据和同步数据，并且将对应于接收到的用户数据的每个衰落校正调节码元路由至反向码元映射器 814，该反向码元映射器 814 执行由每个码元映射器 606-608 执行的功能的相反的功能。即，反向码元映射器 814 与反向码元映射器 276 相类似地操作，并且对对应于解密码元的 P 元组进行恢复，以产生对应于接收到的用户数据的恢复比特流。随后，反向码元映射器 814 将恢复比特流传送到解码器 818，优选地是 FEC 解码器，该解码器与解码器 278 相类似地操作且对恢复比特流进行解码，以产生解码比特流。随后，接收通信设备根据公知的信号处理技术对解码比特流进行进一步处理。此外，与信号处理单元 270 相类似，在本发明的其他实施例中，取决于对应的发射通信设备的特征，信号处理单元 800 可能不包括解码器 818 或者可能进一步包括多个解交织器。

此外，通过向将被经由无线链路发射的多个码元中的每个码元施加相移和幅度调节中的至少其中之一，提供了一种提供物理层加密的发射通信设备 202，其改进了现有技术中无线链路上发射的数据的加密。当同时发射多个数据类型时，例如导频数据、同步数据和用户数据，为了定制每个数据流的加密，发射通信设备可以单独地对每个数据流的码元进行加密。在本发明的另一实施例中，提供一种接收通信

设备，其能够通过每个加密码元施加相移和幅度调节中的至少其中之一从而对加密码元进行解密，其中所述加密码元对应于由发射接收通信设备施加到码元的相移或幅度调节。

尽管已经参考特定的实施例对本发明进行了具体地阐述和显示，但本领域技术人员应该理解的是，在不背离由以下权利要求书所说明的本发明的精神上和范围的情况下，可以作出各种改变和使用等价物对各部件进行替换。此外，本领域技术人员可以意识到，此处详细描述的发射通信设备和接收通信设备的组件与操作不是排他性的，而仅仅是被提供用于帮助理解和评估本发明的创造性原理和优点，而并非用于以任何方式限制本发明。因此，说明和附图都应该被认为是说明性的而非限制性的，且上述变化和替换都应当被视为被包含在本发明的范围之内。

以上已经参考特定实施例描述了本发明的益处、其他优点和解决方案。然而，可以导致任何益处、优点或者解决方案出现或变得更加明确的益处、优点、问题的解决方案和任何部件（多个）都不应被视为是任何或全部权利要求的关键性的、必须的、或本质的特征或部件。如此处使用的，术语“包含”、“包括”或者其任何变型是指覆盖了非排他性的包括，由此，包括一系列部件的工艺、方法、物品、或者装置不仅仅包含那些部件，而且还可以包括没有明确列出的或对于上述工艺、方法、物品、或者装置固有的其他部件。此外，除非此处另有说明，相关联术语的使用，如果有的话，例如第一和第二、顶部和底部等等，在实体或者动作之间不必须需要或暗示任何实际的关系或顺序的情况下，该相关联术语被仅仅用来将这样的一个实体与另一个实体或动作相区别。

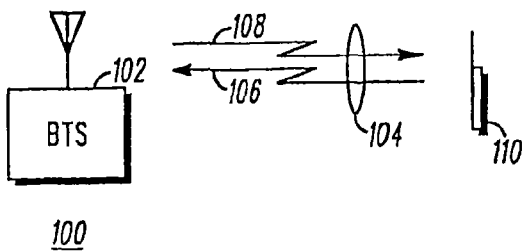


图1

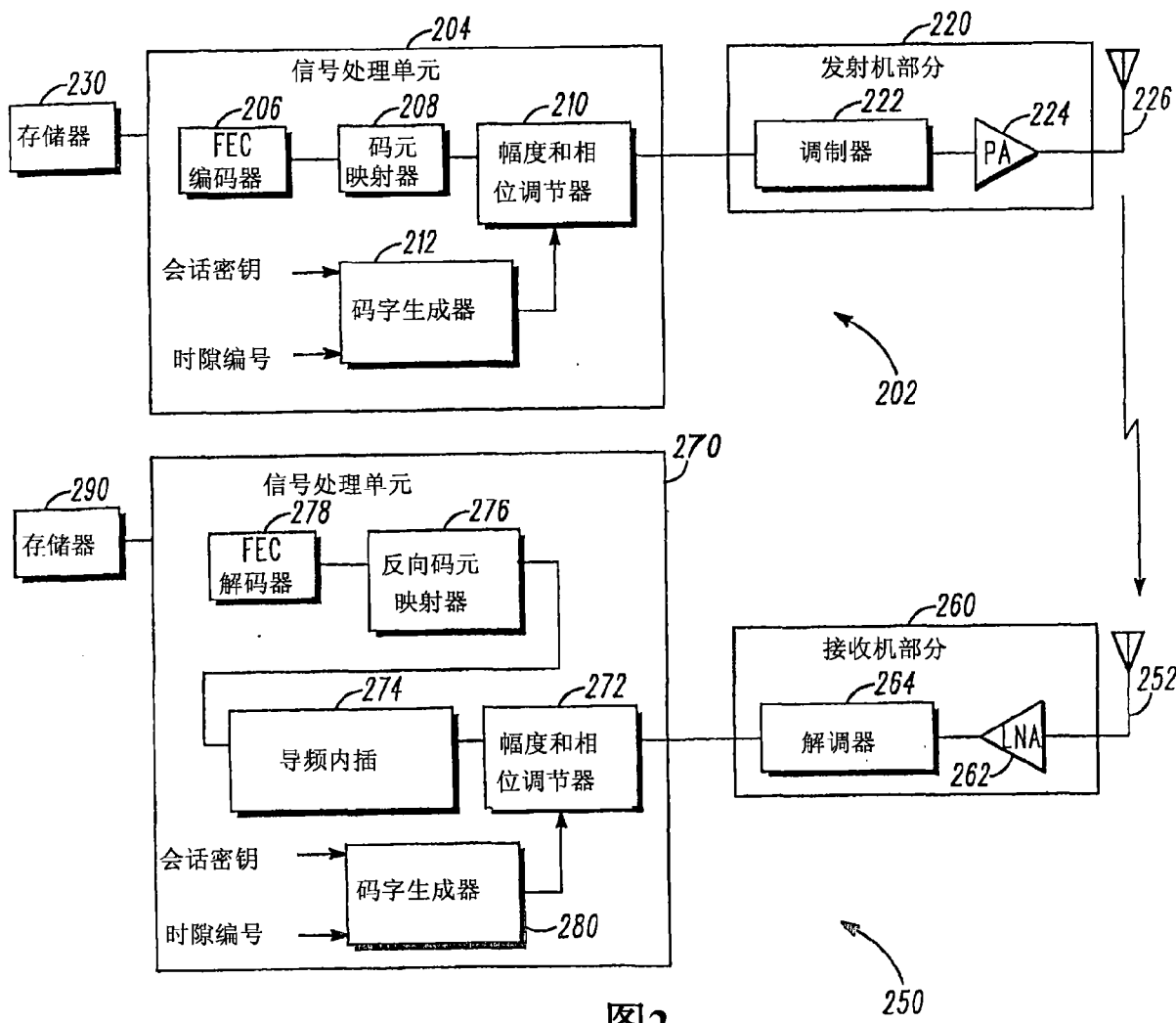


图2

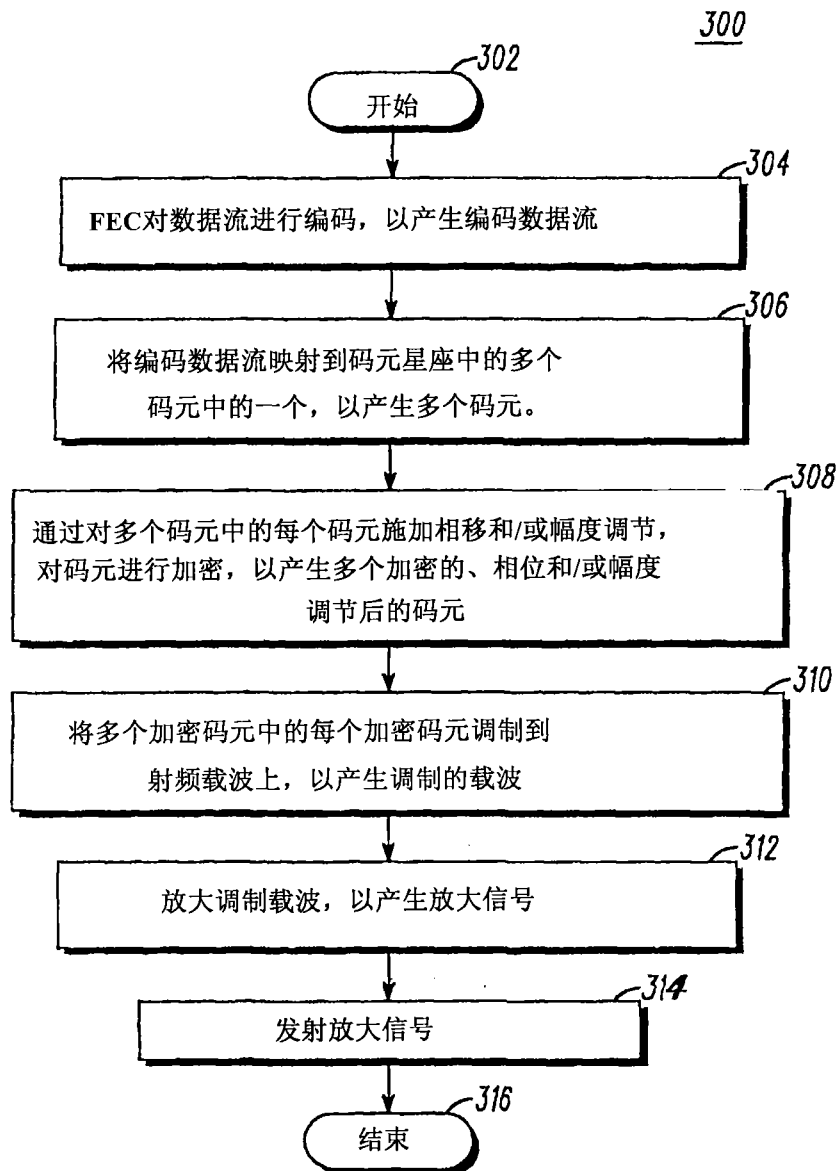


图3

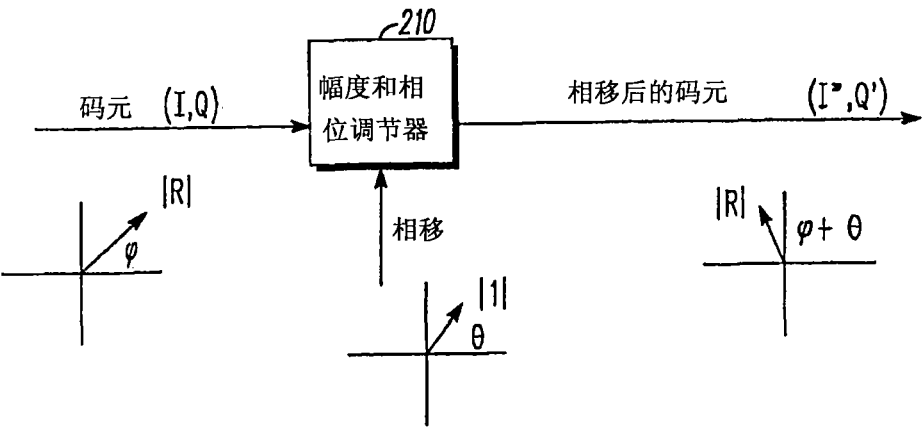


图4

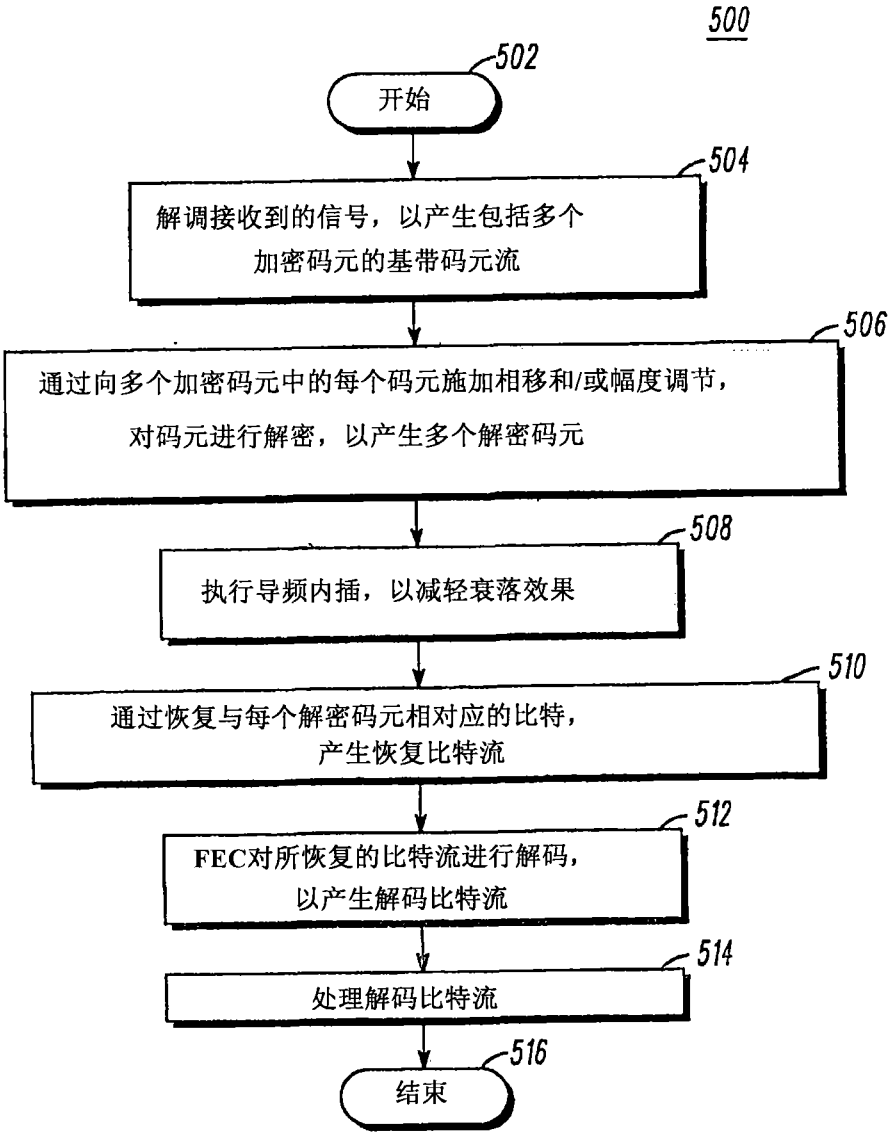


图5

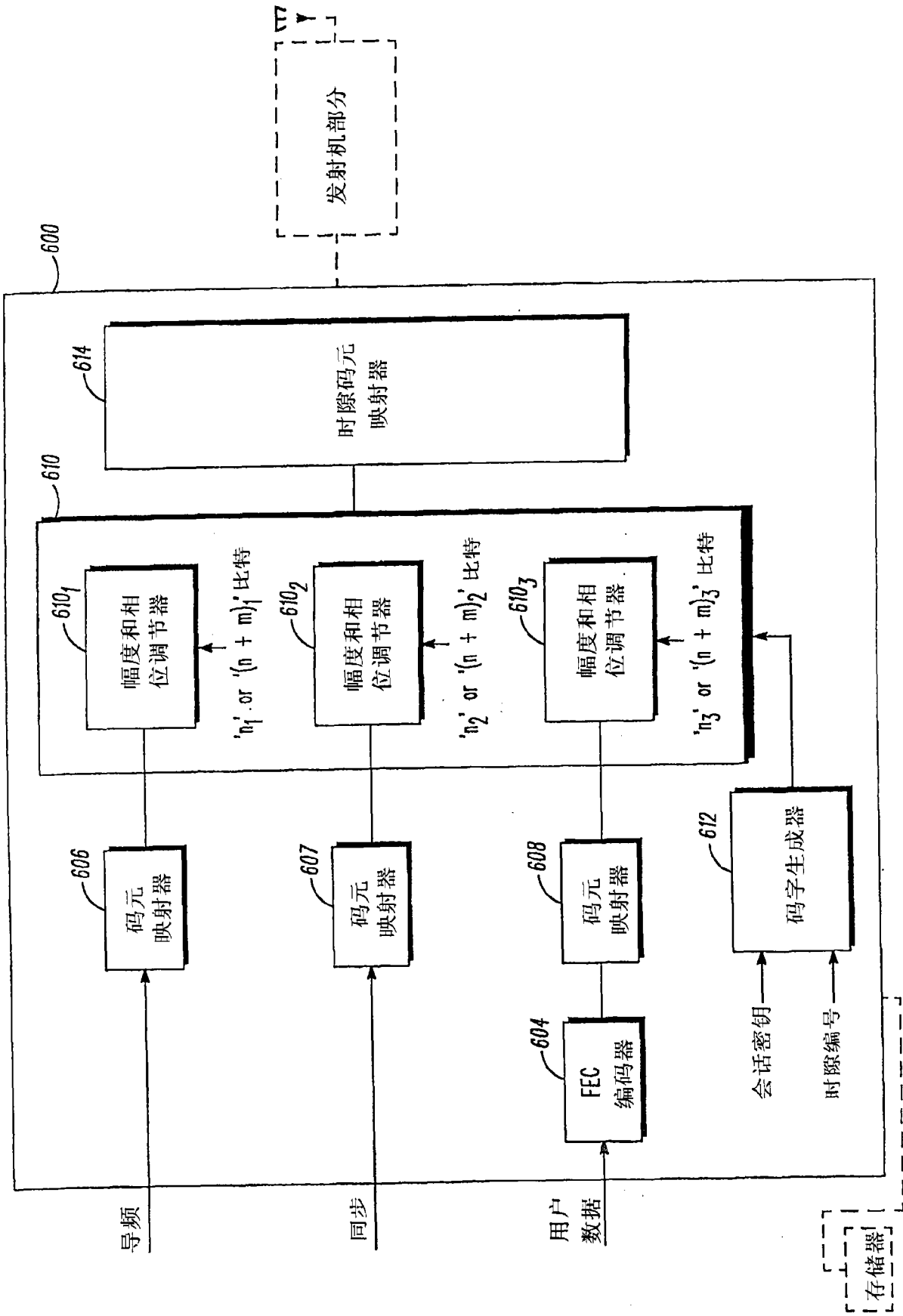
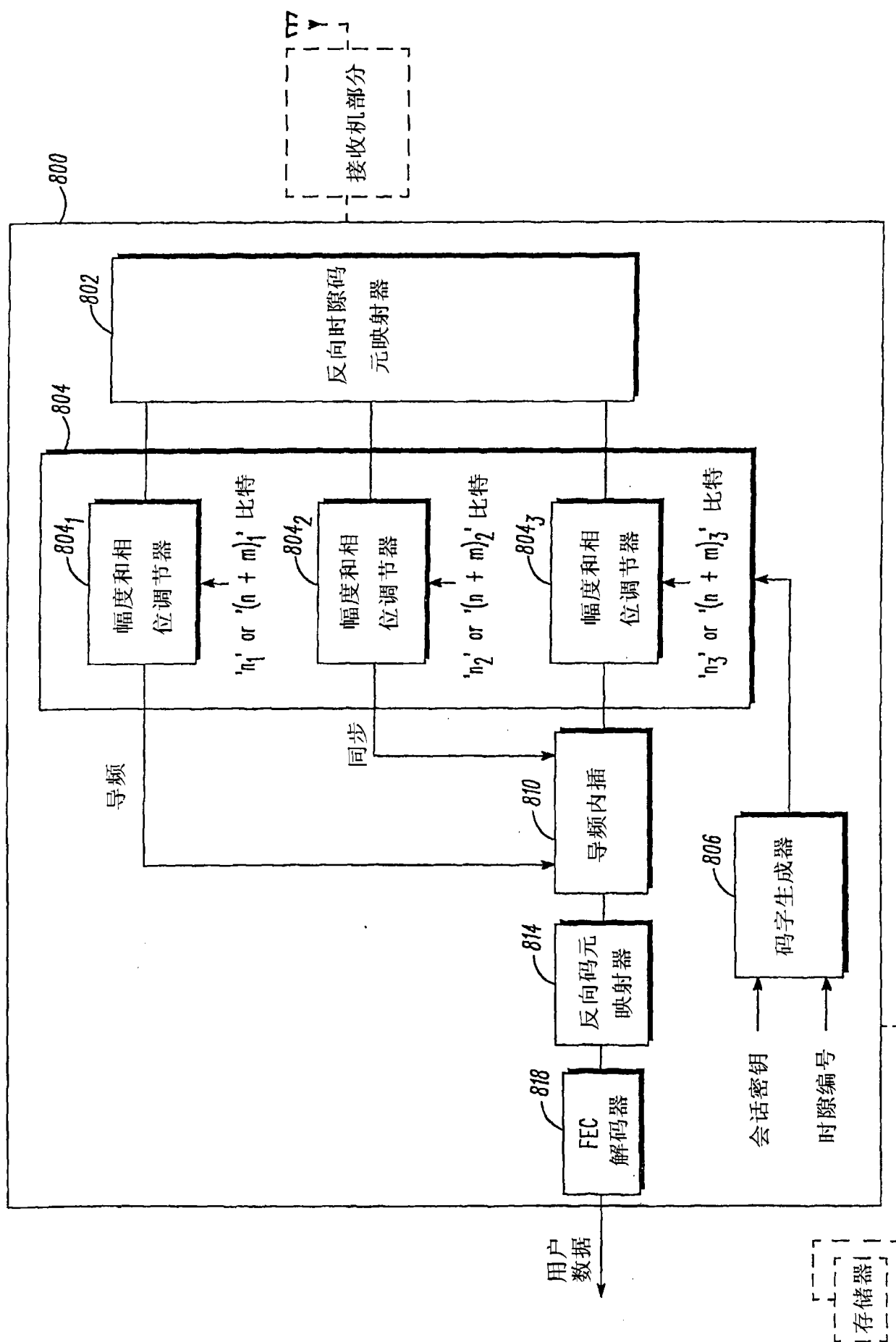


图6

701→ f_1	S	S	S	D	D	D	D	D	P	...
702→ f_2	S	S	S	D	D	P	D	D	D	...
703→ f_3	S	S	S	D	D	P	D	D	D	...
704→ f_4	S	S	S	D	D	D	D	D	P	...

图7



8
冬