

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

H04B 1/04

H04L 9/00 H04K 1/00

[12] 发明专利申请公开说明书

[21] 申请号 98812567.6

[43] 公开日 2001 年 2 月 7 日

[11] 公开号 CN 1283333A

[22] 申请日 1998.12.4 [21] 申请号 98812567.6

[30] 优先权

[32] 1997.12.22 [33] US [31] 08/996,176

[86] 国际申请 PCT/US98/25803 1998.12.4

[87] 国际公布 WO99/33191 英 1999.7.1

[85] 进入国家阶段日期 2000.6.22

[71] 申请人 摩托罗拉公司

地址 美国伊利诺斯

[72] 发明人 沃尔特·李·戴维斯 杰夫·拉维尔

维多利亚·A·莱昂纳多

巴里·W·西罗德

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

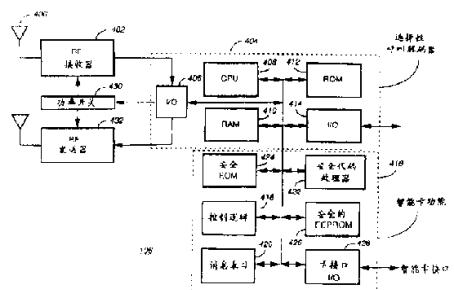
代理人 于 静

权利要求书 4 页 说明书 32 页 附图页数 8 页

[54] 发明名称 便携式双向无线金融消息单元

[57] 摘要

一种便携式双向安全金融消息单元(906)包括接收器(804)、选择性呼叫解码器(1004)、金融交易处理器(1014)、主处理器(1006)和发送器(1034)。选择性呼叫解码器(1004)对接收到的安全金融交易消息进行解码并直接传送到安全金融消息单元中的金融交易处理器(1014)中或智能卡中以防止对安全金融交易消息中包含的信息进行非授权的访问。该便携式双向安全金融消息单元(906)还可能发起和接收金融交易。



权利要求书

1. 一种便携式双向安全金融消息单元，包括：
接收器；
与接收器相耦合的选择性呼叫解码器；
与选择性呼叫解码器相耦合的金融交易处理器；
与金融交易处理器以及选择性呼叫解码器相耦合的主处理器；和
与主处理器相耦合的发送器。
2. 根据权利要求 1 的便携式双向安全金融消息单元，其中金融交易处理器接收和解密来自选择性呼叫解码器的安全金融交易消息。
3. 根据权利要求 2 的便携式双向安全金融消息单元，其中选择性呼叫解码器对接收到的安全金融交易消息进行解码并将其直接传送给金融交易处理器以防止对安全金融交易消息中的信息进行未授权的访问。
4. 根据权利要求 3 的便携式双向安全金融消息单元，其中金融交易处理器对接收到的安全金融交易消息进行解密并将其耦合至用于保持对安全金融交易消息进行解密得到的信息的安全存储器中。
5. 根据权利要求 2 的便携式双向安全金融消息单元，其中安全金融交易消息包括金融交易对话密钥。
6. 根据权利要求 5 的便携式双向安全金融消息单元，其中安全金融交易消息包括返回的现金值。
7. 根据权利要求 5 的便携式双向安全金融消息单元，其中安全金融交易消息包括返回的资金转移值。
8. 根据权利要求 5 的便携式双向安全金融消息单元，其中安全金融交易消息包括返回的信贷值。
9. 根据权利要求 2 的便携式双向安全金融消息单元，其中选择性呼叫解码器对接收到的安全金融交易消息进行解码，并直接传送到相连的智能卡中以防止对安全金融交易消息中包含的信息进行非授权的访问。

10. 根据权利要求 1 的便携式双向安全金融消息单元，包括：
与金融交易处理器以及主处理器相耦合的安全消息发生器。

11. 根据权利要求 10 的便携式双向安全金融消息单元，其中金融
交易处理器加密并且安全消息发生器产生耦合至主处理器以由发送器
进行发送的安全金融交易消息。

12. 根据权利要求 11 的便携式双向安全金融消息单元，其中安全
金融交易消息包括金融交易请求。

13. 根据权利要求 11 的便携式双向安全金融消息单元，其中安全
金融交易消息包括现金装载请求。

14. 根据权利要求 11 的便携式双向安全金融消息单元，其中安全
金融交易消息包括资金转移请求。

15. 根据权利要求 11 的便携式双向安全金融消息单元，其中安全
金融交易消息包括信贷请求。

16. 一种便携式双向安全金融消息单元，包括：

接收器；

与接收器相耦合的选择性呼叫解码器；

与选择性呼叫解码器相耦合的金融交易处理器，该金融交易处理
器包括：

安全代码处理器；

与安全代码处理器相耦合的安全非易失只读存储器；

与安全非易失只读存储器相耦合的安全可擦写只读存储器；

与安全可擦写只读存储器相耦合的输入/输出接口；和

与安全代码处理器、安全非易失只读存储器、安全可擦写只读存
储器以及输入/输出接口相耦合的控制逻辑；

与金融交易处理器和选择性呼叫解码器相耦合的主处理器；以及
与主处理器相耦合的发送器。

17. 根据权利要求 16 的便携式双向安全金融消息单元，包括：
通过输入/输出接口和金融交易处理器相耦合的智能卡。

18. 根据权利要求 16 的便携式双向安全金融消息单元，其中金融

交易处理器接收和解密来自选择性呼叫解码器的安全金融交易消息。

19. 根据权利要求 18 的便携式双向安全金融消息单元，其中选择性呼叫解码器对接收到的安全金融交易消息进行解码并将其直接传送给金融交易处理器以防止对安全金融交易消息中的信息进行未授权的访问。

20. 根据权利要求 19 的便携式双向安全金融消息单元，其中金融交易处理器对接收到的安全金融交易消息进行解密并将其耦合至用于保持对安全金融交易消息进行解密得到的信息的安全存储器中。

21. 根据权利要求 18 的便携式双向安全金融消息单元，其中安全金融交易消息包括金融交易对话密钥。

22. 根据权利要求 21 的便携式双向安全金融消息单元，其中安全金融交易消息包括返回的现金值。

23. 根据权利要求 21 的便携式双向安全金融消息单元，其中安全金融交易消息包括返回的资金转移值。

24. 根据权利要求 21 的便携式双向安全金融消息单元，其中安全金融交易消息包括返回的信贷值。

25. 根据权利要求 18 的便携式双向安全金融消息单元，其中选择性呼叫解码器对接收到的安全金融交易消息进行解码，并直接传送到相连的智能卡中以防止对安全金融交易消息中包含的信息进行非授权的访问。

26. 根据权利要求 16 的便携式双向安全金融消息单元，包括：与金融交易处理器以及主处理器相耦合的安全消息发生器。

27. 根据权利要求 26 的便携式双向安全金融消息单元，其中金融交易处理器加密并且安全消息发生器产生耦合至主处理器以由发送器进行发送的安全金融交易消息。

28. 根据权利要求 27 的便携式双向安全金融消息单元，其中安全金融交易消息包括金融交易请求。

29. 根据权利要求 27 的便携式双向安全金融消息单元，其中安全金融交易消息包括现金装载请求。

30. 根据权利要求 27 便携式双向安全金融消息单元，其中安全金融交易消息包括资金转移请求。
31. 根据权利要求 27 便携式双向安全金融消息单元，其中安全金融交易消息包括信贷请求。

说 明 书

便携式双向无线金融消息单元

本发明一般涉及选择性呼叫信令系统，更特别地，涉及使用一个便携式单向金融消息单元经过一个无线网络方便地实现安全金融交易的一个选择性呼叫信令系统。

在传统的选择性呼叫信令系统中，一个用户或者发起者可能向一个用户单元（例如，选择性呼叫接收器）发送一个消息，这个消息包括与这个用户单元相关的一个地址和数据。这个数据可以是一种形式，也可以是多种形式，例如表示一个电话号码的数字，表示一个可阅读的文本消息的字母字符，或者可能是包括音频和图形信息的一个多媒体消息。典型地，这个消息的形式足够传送个人之间的信息，或者传送与他们的商务，特殊的兴趣，在哪里，一般的时间安排，或者时间要求严格约会相关的服务。但是，由于社会要求在人们移动时可得到更多的信息，所以必须找到一个方法来允许一个人进行个人的或者商务交易，并且能够被通知其个人事件，谈判，和商业信息，而不会失去联系。

考虑传统的无线系统，包括蜂窝和寻呼应用，为了实现可靠的和私有的个人的或者商务交易以前，它必须要解决许多重要问题。因为工程科学的进步，特别是在无线通信和计算机科学领域内的进步，对一个“电脑黑客”来说，已经比较容易来监视被广播到这个选择性呼叫接收器的地址和数据了。这个不希望有的监视或者偷听就对无线通信系统的一个潜在用户提出了一个问题，即，他们的个人数据可能被未授权个人获取，这样如果广播了秘密信息的话，就对双方产生了一个不必要的危险。另外，如果这个信息包括表示一个个人地址，序列号，个人标识号码（PIN）或者类似信息的明文数据，监视这个数据流的一个不道德者就可以访问一个个人的私有帐号，或者非法盗用这个地址来复制一个没有授权的通信装置。使用这个方法来偷盗服务或

者秘密信息可能是现在的和将来的通信设备制造商和服务提供者所面临的、最使人畏缩的问题。在电子金融交易领域内，特别关注如何确保广播中所包括的数据的安全。包括在一个金融交易中的明文数据很容易被他人获取，并且将引起而且也肯定会产生对基金的盗用或者对一个人的欺诈行为。

这样，所需要的是这样一个无线消息系统，它能够允许一个通信发起者在一个用户单元和这个发起者之间进行一个安全的消息通信，并且鉴别这个安全的消息，而不暴露这个消息的内容或者含义。

简而言之，根据本发明，提供了用于使用寻呼协议，例如 FLEXTM (Motorola 公司的一个商标)、POCSAG (邮政编码标准化顾问组) 或者类似的协议，经过已有的寻呼基础设施设备来发送包括安全金融交易的数据的一个方法和装置。

本发明的第一方面涉及实现一个硬件来实现用于将安全的消息覆盖在一个已有寻呼基础设施之上的一种方法。这个已有寻呼基础设施包括一个寻呼终端，这个寻呼终端包括用于处理所接收的消息和它们相应目的请求的一个寻呼编码器。这个寻呼终端产生包括所接收的消息和它们相应的选择性呼叫地址 (从相应的目的请求判断出来的) 的一个选择性呼叫消息的消息队列。这个寻呼终端处理对这个消息队列中选择性呼叫消息的分发，这个寻呼终端将这些消息分发到至少一个基站 (例如，发送器，天线，和接收器) 以在这个基站和这个用户单元或者寻呼机之间进行通信。

本发明的第二方面涉及将一个密码引擎放置在这个寻呼终端中，以选择性地对从一个通信发起者和从这个用户单元或者寻呼机接收的消息进行加密，解密，签名，和证实这些消息的可靠性。

本发明的第三方面涉及配备了一特殊安全模块的这个用户单元或者寻呼机，这个特殊的安全模块能够处理包括在这个选择性呼叫消息中的加密信息，来证实它们的可靠性和真实性，提取被加密的数据，并且如果需要的话返回被加密的响应或者确认，来鉴别和证实对安全消息的接收。

本发明的第四方面涉及配备了一个基本装置和可能配置一个第二装置的用于交换向内和向外消息的这个用户单元或者寻呼机。这个基本装置包括一个传统的无线频率接收器和可选地包括一个传统的无线频率发送器。这个第二装置包括一个光接收器和可选地一个光发送器。替代地，这个第二装置进一步包括一个或者多个声波换能器或者其它的电磁换能器和相关的电路结构，以在这个用户单元或者寻呼机与发起者之间实现一个单向的或者双向的通信链路。

本发明的第五方面涉及用户单元或者寻呼机，这个用户单元或者寻呼机包括与一个电子金融卡或者资金储蓄卡，借记卡，信用卡，或者银行帐号中至少一个相应的一个、预定的帐号标识。

本发明的第六方面涉及用户单元或者寻呼机，这个用户单元或者寻呼机包括与电子金融卡或者资金储蓄卡，借记卡，信用卡，或者银行帐号中至少两个相应的多个、预定的帐号标识。

本发明的第七方面涉及在这个寻呼终端中的这个密码引擎和这个用户单元或者寻呼机中的、包括多个密码过程的安全模块。这些加密过程包括私钥和公钥系统，如果合适的话。一个这样的私钥系统是使用 CBC 模式中的 ANSI X3.92 DES 算法的数据加密标准 (DES)。类似地，一第一公钥系统是 RSA (由 Rivest, Shamir, 和 Adleman 发明的)，一种基于使用模数 n 整数乘法和乘幂实现的亚指数单向函数的一个密码过程。一第二公钥系统使用椭圆曲线技术，一种基于在有限字段内实现的、高度非线性指数单向函数的密码过程。

本发明的第八方面涉及从这个用户单元或者寻呼机发起一个无线交易，这个无线交易与一个电子金融卡或者资金储蓄卡，借记卡，信用卡，或者银行帐号中至少一个相关。

本发明的第九方面涉及一个用户选择的个人标识号码，它可以被编程到这个用户单元或者寻呼机中，以保护装载在这个用户单元或者寻呼机内的金融帐号或者资金。

本发明的第十方面涉及一个用户选择的个人标识号码，它可以经过这个用户单元或者寻呼机被编程到智能卡中，这样就不能够访问被

保护智能中的任何细节，除非在这以后被这个用户单元或者寻呼机所访问或者被重新编程。

本发明的第十一个方面涉及将一个授权用户单元或者寻呼机鉴别为这个无线金融交易的一个通信代理，并且当一个向内的或者向外的金融交易在一个发起者和一个没有授权用户单元或者寻呼机之间进行时，选择性地不允许任何到属于或者被这个授权用户单元或者寻呼机所控制的帐号的金融交易，和替代地，禁止超过被一个授权用户或者一个调控者，例如一个银行、一个信用卡发行商等，所设置的一个预定限度的资金转移或信用卡交易。

图 1 是根据本发明的优选实施方式所使用的、一个数据传送系统的一个电路框图。

图 2 是根据本发明的优选实施方式用于处理和发送消息信息的一个电路框图。

图 3-5 是显示根据本发明的优选实施方式而使用的信令协议的发送格式的时序图。

图 6 和 7 是显示根据本发明的优选实施方式而使用的同步信号的时序图。

图 8 是根据本发明的优选实施方式的一个金融消息单元的一个电路框图。

图 9 是根据本发明的一个安全消息系统的一个图。

图 10 是根据本发明的优选实施方式的一个金融消息单元的一个高层框图。

图 11 是可以被用于一个金融组织的前端设备上、来经过一个寻呼信道将安全电子资金转移授权发送到金融消息单元的消息组成和加密设备的一个框图。

图 12 是一个无线选择性呼叫信令系统控制器的一个功能图，这个无线选择性呼叫信令系统控制器实现了能够与金融消息单元进行信令通信的一个混合单向和双向安全消息系统的。

图 13 使用一个类似于在电子工业中众所周知的国际标准组织

(OSI) 协议栈图的格式，描述了一个消息系统的各层。

图 14 是描述根据本发明的优选实施方式的一个金融消息单元的典型操作的一个流图。

图 15 显示了与通过和从一个无线金融消息单元，请求和授权资金的电子转移或者资金的借贷相关的一个典型序列。

图 16 显示了在一个单向和一个双向安全通信系统中，与通过和从一个无线金融消息单元的，资金的无线转移或者资金的借贷相关的一个典型序列。

参考图 1，图 1 显示了根据本发明的优选实施方式所使用的一个数据传送系统 100，例如一个寻呼系统的一个电路框图。在这个数据传送系统 100 中，或者是从一个电话（与提供数字数据传送的一个系统中相同）或者从一个消息输入装置例如一个字母数字数据终端发起的消息，通过公众交换电话网络（PSTN）被路由到一个寻呼终端 102，这个寻呼终端 102 处理被这个系统内所提供的一个或者多个发送器 104 所传送的数字或者字母消息信息。当使用多个发送器时，这个发送器 104 优选地使用同时联播将这个消息信息发送到金融消息单元 106。下面描述这个寻呼终端 102 对数字和字母信息进行的处理，和传送这个消息所使用的协议。

参考图 2，图 2 显示了根据本发明的优选实施方式，用于处理和控制消息信息的发送的寻呼终端 102 的一个电气框图。短消息，例如可以使用一个 Touch-Tone (按键式)™ 电话而随意输入的单音频消息和数字消息，以该领域内众所周知的方式，通过一个电话接口 202 连接到这个寻呼终端 102。较长的消息，例如需要使用一个数据输入装置的字母数字消息，通过使用很多众所周知的调制解调器传送协议中的任何一个的一个调制解调器 206 连接到这个寻呼终端 102。当接收到发送一个消息的一个呼叫时，一个控制器 204 处理这个消息的处理。这个控制器 204 优选是一个微计算机，例如由 Motorola 公司制造的一个 MC680x0 或者等效的微计算机，并且这个微计算机运行很多预编程的例程，例如控制象语音提示等这种终端操作，来引导这个呼叫发

起者输入消息，或者控制握手协议以从一个数据输入装置接收消息。当接收到一个呼叫时，这个控制器 204 参考被保存在用户数据库 208 中的信息，以决定如何处理正在被接收的这个消息。用户数据库 208 包括，但是不局限于，例如被分配到金融消息单元的地址信息，与这个地址相关的消息类型，和与这个金融消息单元的状态相关的信息，例如激活或者因为付费问题而处于非激活状态。提供了连接到这个控制器 204 的一个数据输入终端 240，这个数据输入终端 240 可以用于输入数据，更新和删除被保存在用户数据库 208 中的信息，用于监视系统的性能，和用于获得例如计费信息等这样的信息。

用户数据库 208 也包括这样的信息，例如关于这个金融消息单元被分配了什么传输帧和什么传输状态的信息，这在下面将进一步详细描述。被接收的消息被保存在一个激活页文件 210 中，这个激活页文件 210 根据被分配到金融消息单元的传输状态，以队列的形式保存消息。在本发明的优选实施方式中，在激活页文件 210 中提供了 4 个状态队列。这个激活页文件 210 优选是一个双端口先进先出的随机访问存储器，但是，应理解，也可以使用其它形式的随机访问存储器装置，例如硬盘驱动器。在控制器 204 的控制下，使用一个实时时钟 214 或者其它合适的定时源所提供的定时信息，周期性地从激活页文件 210 中恢复被保存在每一个状态队列中的消息信息。从每一个状态队列中恢复的消息信息被以帧号码进行排序，然后根据地址、消息信息和如何其它传输所需要的信息（所有这些均称作与消息相关的信息）来进行组织，然后由帧分批控制器 212 根据消息的大小来这些信息批处理成帧。每一个状态队列的成批帧信息被连接到帧消息缓冲器 216，帧消息缓冲器 216 用于临时保存成批帧信息，直到对这些信息进行进一步的处理和发送。帧被以数字序列进行分批，所以虽然正在发送一个当前帧，但是需要被发送的下一帧在帧消息缓冲器 216 中，其后的下一帧被检索和进行批处理。在合适的时刻，保存在帧消息缓冲器 216 中的成批帧消息被传送到帧编码器 218，又保持状态队列的关系。帧编码器 218 将地址和消息消息编码成需要进行传输的地址和消息码

字，如下面将要描述的。被编码的地址和消息码字被排序成块，然后连接到，最好一次交织 8 个码字来形成交织传输信息块的一个块交织器 220，以便按业内周知的方式进行传输。包括在被每一个块交织器 220 所产生的交织信息块中的交织码字然后被串行地传送到一个状态复用器 221，这个状态复用器 221 将这个消息信息一个比特一个比特地复用成一个传输状态下的一串行数据流。接着，这个控制器 204 使能一个帧同步产生器 222，这个帧同步产生器 222 产生在每一个帧传输的开始处被发送的同步码字。在控制器 204 的控制下，串行数据融合器 224 将这个同步码字与地址和消息信息复用在一起。并且从其产生适合于进行传输的格式下的一个消息流。接着，这个消息流连接到一个发送器控制器 226，这个发送器控制器 226 在控制器 204 的控制下经过一个分布式信道 228 发送这个消息流。这个分布式信道 228 可以是众所周知的一些信道中的任何一个，例如一个有线、一个 RF 或者微波分布式信道，或者一个卫星分布式信道。这个分布式消息流被传送到一个或者多个发送器站 104，这与通信系统的大小有关。首先，这个消息流被传送到用于临时保存发送前的消息流的一个双端口缓冲器 230。在定时和控制电路 232 所决定的一个合适的时刻，这个消息流被从这个双端口缓冲器 230 中恢复，并且连接到一个最好为 4 电平 FSK 调制器 234 的输入端。然后，这个被调制的消息流连接到发送器 236，以经过天线 238 进行发送。

参考图 3, 4 和 5，这些时序图显示了根据本发明的优选实施方式所使用的信令协议的发送格式。这个信令协议通常称作 MotorolaTM 的 FLEXTM 选择性呼叫信令协议。如图 3 所显示的，这个信令协议使消息被发送到金融消息单元，例如寻呼机，寻呼机被分配了标号为帧 0 到帧 127 的 128 帧中的一个或者多个帧。然后，应理解，信令协议中所提供的实际帧数目可以比上述数目多或者少。所使用的帧数目越大，可以被提供到在这个系统中工作的金融消息单元的电池寿命就越长。使用的帧数目越少，消息就更经常地被排队和发送到被分配了任何特定帧的金融消息单元，由此减少了等待时间或者发送消息所需的时间。

如图 4 所显示的，帧包括一个同步码字（sync），其后最好是标号为块 0 到块 10 的 11 个消息信息块（信息块）。如图 5 所显示的，每一个消息消息块最好包括 8 个地址、控制或者数据码字，它们在每一个状态的编号为 0 到 7。所以，一个帧中的每一个部分允许发送 88 个地址、控制和数据码字。优选地，地址、控制和数据码字包括两个集合，一第一集合涉及包括一短地址矢量，一长地址矢量，一第一消息字，和一空词的一个矢量字段，一第二集合涉及包括一个消息字和一个空字的一个消息字段。

优选地，地址、控制和数据或者消息码字是 31, 21BCH 码字，其中一添加的第 32 偶校验比特提供了到码字集合的一个额外的比特距离。应理解，其它码字，例如 23, 12 戈雷码字也可以被使用。在众所周知的 POCSAG 信令协议中，使用了第一码字比特来定义码字类型，如地址或者数据，来提供地址和数据码字，与 POCSAG 协议不同，在根据本发明的优选实施方式而使用的 FLEX™ 信令协议中，地址和数据码字之间没有这样明确的区分。地址和数据码字而是通过它们在每独立帧中的位置来定义的。

图 6 和 7 是显示根据本发明的优选实施方式而使用的同步码字的时序图。特别地，如图 6 所显示的，同步码字优选包括 3 个部分：一第一同步码字（sync 1），一个帧信息码字（帧信息）和一第二同步码字（sync 2）。如图 7 所显示的，这个第一同步码字包括标识为比特同步 sync 1 和 BS1 的、用于提供比特同步的 0 和 1 交替的比特图形的第一和第三部分，和标识为“A”和其补“A 杠”的、用于提供帧同步的第二和第四部分。第二和第四部分优选是预定义的来提供高码字相关可靠性，并且也用于指示地址和消息被发送的数据比特速率的单个 32, 21BCH 码字。表 1 定义了和信令协议一起使用的数据比特速率。

比特率	“A”值
1600bps	A1 和 A1 杠
3200bps	A2 和 A2 杠
6400bps	A3 和 A3 杠

没有定义	A4 和 A4 杠
------	-----------

表 1

如表 1 所显示的，3 个用于发送地址和消息的数据比特率被与预定义了，但是应理解，也可以预定义更多或者更少的数据比特率，这与系统的需求相关。

优选地，帧信息码字是在数据部分中包括一预定数目的、用于预留来标识帧号码的比特，例如 7 个比特来标识帧号码为 0 到帧号码 127 的一个单个 32, 21BCH 码字。

优选地，第二同步码字的结构与上述第一同步码字的结构类似。但是，与优选使用一固定数据符号速率，例如 1600bps（每秒比特）来进行发送的第一同步码字不同，第二同步码字以地址和消息需要在任何给定帧中被发送的数据符号速率来进行发送。所以，第二同步码字允许金融消息单元在帧发送数据比特速率上，获得“精细”的比特和帧同步。

总之，根据本发明的优选实施方式而使用的信令协议包括 128 帧，128 帧包括一预定义同步码字，其后是 11 个包括每一个阶段的地址、控制或者消息码字的信息块。这个同步码字能够标识数据发送速率，并且通过使金融消息单元以变化的发送速率来发送数据码字确保金融消息单元的同步。

图 8 是根据本发明的优选实施方式的金融消息单元 106 的一个电路框图。这个金融消息单元 106 的心脏是一个控制器 816，这个控制器 816 优选使用一个低功耗的 MC68HC0x 微计算机，例如 Motorola 公司所制造的，或者类似的微计算机来实现。这个微计算机控制器，从其后称作控制器 816，接收和处理从一些外设电路输入的输入，例如图 8 所示，并且使用软件子例程来控制外设电路的操作和交互。使用用于处理和控制功能（例如，作为一个功能控制器）的一个微计算机控制器对该领域内的一个普通技术人员来说很熟悉的。

金融消息单元 106 能够接收优选使用 2 电平和 4 电平频率调制技术来进行调制的地址、控制和消息信息，其以下称作“数据”。被发送

的数据被连接到一个接收器部分 804 的输入的的一个天线 802 所接收。接收器部分 804 以该领域内一个众所周知的方式来处理被接收的数据，在输出端提供一个模拟 4 电平恢复数据信号，其以下称作一个被恢复的数据信号。被恢复的数据信号连接到一个阈值电平提取电路 808 的一个输入，和连接到一个 4 电平解码器 810 的一个输入。

参考 Kuznicki 等等所发表的、其受让人是 Motorola 公司的美国专利号 No., 282, 205、题为“提供变长消息携带及其方法的数据通信终端”，可以更好地理解在图 8 的金融消息单元中所描述的阈值电平提取电路 808 的操作，4 电平解码器 810 的操作，符号同步器 812 的操作，4 电平到二进制转换器 814，同步码字相关器 818 和状态定时产生器（数据恢复定时电路）826。这里，这个专利的思想被用作参考。

再参考图 8，阈值电平提取电路 808 包括具有用作被恢复数据信号的输入的两个时钟电平检测器电路（没有显示）。优选地，17%，50% 和 83% 的信号状态被使用来对被提供到这个阈值电平提取电路 808 的 4 电平数据信号进行解码。

当功率开始加到接收器部分时，如当首先打开这个金融消息单元时，通过一个控制输入（中心采样）预设置了一个时钟速率选择器，以选择一个 128 倍的时钟，即频率是最慢的数据比特率，即上面所描述的 1600bps 的 128 倍的一个时钟。如图 8 所显示的，这个 128 倍的时钟是由 128 倍时钟产生器 844 所产生的，这个时钟产生器 844 优选是工作频率为 204.8KHz（千赫兹）的一个晶体控制振荡器。128 倍时钟产生器 844 的输出被连接到分频器 846 的一个输入，以将输出频率除以 2 来产生一个工作在 102.4KHz 的一个 64 倍时钟。这个 128 倍时钟允许电平检测器在一个非常短的时间内，异步地检测信号的峰值幅度和谷值幅度，由此产生进行调制解码时所需要的低（Lo），平均（Avg），和高（Hi）阈值输出信号值。在与同步信号进行了符号同步后，如下面将要描述的，这个控制器 816 产生一第二控制信号（中心采样），来选择如图 8 所显示的、由符号同步器所产生的一个 1 倍符号时钟。

优选地，4 电平解码器 810 使用 3 个电压比较器和一个符号解码器来进行工作。被恢复的数据信号连接到其阈值与归一化信号状态的 17%，50% 和 83% 相应的 3 个比较器的一个输入。通过将被恢复的数据信号连接到一个 83% 比较器的第二输入，一个 50% 比较器的第二输入，和一个 17% 比较器的第二输入，所产生的系统有效地恢复被解调的 2- 或者 4- 电平 FSK 信息信号。与低 (Lo)，平均 (Avg)，和高 (Hi) 阈值输出信号值相应的 3 个比较器的输出连接到一个符号解码器的输入。然后，这个符号解码器根据表 2 来对输入进行解码。

阈值			输出	
Hi	Avg	Lo	MSB	LSB
$RC_{in} <$	$RC_{in} <$	$RC_{in} <$	0	0
$RC_{in} <$	$RC_{in} <$	$RC_{in} >$	0	1
$RC_{in} <$	$RC_{in} >$	$RC_{in} >$	1	1
$RC_{in} >$	$RC_{in} >$	$RC_{in} >$	1	0

表 2

如表 2 所显示的，当被恢复的数据信号 (RC_{in}) 比所有 3 个阈值均小时，所产生的符号是 00 (MSB = 0, LSB = 0)。所以，当超过 3 个阈值中的每一个时，就产生一个不同的符号，如上面的表 2 所显示的。

从 4- 电平解码器 810 输出 的 MSB 输出被连接到这个符号同步器 812 的一个输入，并且提供通过检测在 4- 电平被恢复数据信号中的过零而产生的一个被恢复数据输入。被恢复数据输入的正电平表示模拟 4- 电平被恢复数据信号在平均阈值输出信号上的两个正偏移幅度，负电平表示这个模拟 4- 电平被恢复数据信号低于平均阈值输出信号的两个负的偏移幅度。

这个符号同步器 812 使用被分频器 846 所产生的、工作在 102.4KHz 的一个 64 倍时钟，它连接到一个 32 倍速率选择器（没有显示）的一个输入。优选地，这个 32 倍速率选择器是提供可以选择除以 1 或者 2，以产生速率是符号发送速率的 32 倍的一个采样时钟的一个分频器。一

一个控制信号 (1600/3200) 连接到这个 32 倍速率选择器的一第二输入，并且被用于选择符号传送速率为每秒 1600 和 3200 符号中的采样时钟速率。被选择的采样时钟连接到 32 倍数据过采样器 (没有显示) 的一个输入，这个 32 倍数据过采样器以每个符号 32 个采样的速率对被恢复数据信号 (MSB) 进行采样。这个符号采样被连接到当检测到一个符号边缘时产生一个输出脉冲的一个数据边缘检测器 (没有显示)。这个采样时钟也连接到一个 16/32 分频器电路 (没有显示) 的一个输入，这个 16/32 分频器电路用于产生与被恢复数据信号同步的 1 倍和 2 倍符号时钟。优选地，这个 16/32 分频器电路是一个向上/下的计数器。当这个数据边缘检测器检测到一个符号边缘时，就产生一个脉冲，这个脉冲被一个与门与这个 16/32 分频器电路的当前计数进行选通。同时，这个也连接到 16/32 分频器电路的一个输入的数据边缘检测器产生一个脉冲。当连接到这个与门的输入的这个脉冲在 16/32 分频器电路产生一个 32 的计数以前到来时，这个与门所产生的输出就促使 16/32 分频器电路的计数增加 1 个计数，以对从数据边缘检测器连接到 16/32 分频器电路的输入的这个脉冲作出响应。另外，当连接到与门的输入的这个脉冲在 16/32 分频器电路产生一个 32 的计数后到来时，与门所产生的输出就促使 16/32 分频器电路的计数推迟 1 个计数，以对从数据边缘检测器连接到 16/32 分频器电路的输入的这个脉冲作出响应，由此使 1 倍和 2 倍符号时钟与被恢复数据信号进行同步。从下面的表 3 可以更好地理解所产生的这个符号时钟速率。

输入时钟 (相对)	控制输入 (SPS)	速率选择器 分频比例	速率选择 器输出	2 倍符号 时钟 (BPS)	1 倍符号 时钟 (BPS)
64 倍	1600	除以 2	32 倍	3200	1600
64 倍	3200	除以 1	64 倍	6400	3200

表 3

如上面的表所显示的，这个 1 倍和 2 倍符号时钟产生每秒 1600, 3200 和 6400 比特的速率，并且与被恢复数据信号同步。

4- 电平二进制转换器 814 将这个 1 倍符号时钟连接到一时钟速率选择器（没有显示）的第一时钟输入。一个 2 倍符号时钟连接到这个时钟速率选择器的第二时钟输入。这个符号输出信号（MSB, LSB）连接到一个输入数据选择器（没有显示）的输入。一个选择器信号（2L/4L）连接到这个时钟速率选择器的一个选择器输入和这个输入数据选择器的选择器输入，并且提供对作为 2- 电平 FSK 数据或者 4- 电平 FSK 数据的符号输出信号的转换控制。当选择了这个 2- 电平 FSK 数据转换（2L）时，仅选择这个 MSB 输出，这个 MSB 输出连接到一个传统的并行到串行转换器（没有显示）的输入。这个 1 倍时钟输入被时钟速率选择器所选择，这使在并行到串行转换器的输出产生一单比特二进制数据流。当选择了这个 4- 电平 FSK 数据转换（4L）时，选择这个 MSB 和 LSB 输出，这些 MSB 和 LSB 输出连接到一个传统的并行到串行转换器（没有显示）的输入。这个 2 倍时钟输入被时钟速率选择器所选择，这使在并行到串行转换器的输出产生一串行的 2 比特二进制数据流，其速率是 2 倍符号速率。

再参考图 8，被 4- 电平二进制转换器 814 所产生的串行二进制数据流连接到一个同步码字相关器 818 和一个解复用器 820 的输入。这个控制器 816 从一个码存储器 822 中恢复预定的“A”码字同步图形，并且这个预定的“A”码字同步图形连接到一个“A”码字相关器（没有显示）。当所接收的这个同步图形在一个可接受的错误限度内与预定的“A”码字同步图形之一匹配时，就产生一个“A”或者“A-杠”的输出，并且这个输出连接到控制器 816。这个相关的特定“A”或者“A-杠”码字同步图形提供了帧 ID 码字开始的帧同步，并且也定义了后面消息的数据比特速率，如前面所描述的。

这个串行二进制数据流也连接到帧码字解码器（没有显示）的一个输入，这个帧码字解码器对帧码字进行解码，并且提供当前正在被控制器 816 所接收的帧号码的一个指示。在获取同步的期间，例如在打开初始接收器后，电源被电池节电电路 848 提供到接收器部分，如图 8 所显示的，这就可以如上所描述的、接收“A”同步码字，并且

继续提供电源，以处理同步码的余下部分。这个控制器 816 将当前正在接收的帧号码与保存在码存储器 822 中的一个分配帧号码列表进行比较。如果当前正在接收的帧号码与一个被分配的帧号码不同，这个控制器 816 产生连接到电池节电电路 848 的一个输入的一个电池节电信号，这个信号就暂停对接收器部分的电源供电。暂停电源供电直到下一个分配到这个接收器的帧，在这个时刻，这个控制器 816 产生连接到电池节电电路 848 的一个电池节电器信号，以对接收器部分进行供电，来接收被分配的帧。

这个控制器 816 从一个码存储器 822 中恢复一个预定的“C”码字同步图形，并且这个预定的“C”码字同步图形连接到一个“C”码字相关器（没有显示）。当所接收的同步图形在一个可接受的错误限度内与这个预定的“C”码字同步图形匹配时，就产生连接到控制器 816 的一个“C”或者“C-杠”输出。这个特定的、相关“C”或者“C-杠”同步码字提供了到这个帧的数据部分的“精细”帧同步。

通过这个控制器 816 产生连接到一个码字去交织器 824 的输入和一个数据恢复定时电路 826 的输入的一个块开始信号（Blk 开始），就建立了实际数据部分的开始。一个控制信号（2L/4L）连接到或者选择 1 倍或者选择 2 倍符号时钟输入的时钟速率选择器（没有显示）的一个输入。这个被选择的符号时钟连接到一个状态产生器（没有显示）的输入，这个状态产生器优选是被时钟触发来产生 4 个状态输出信号（ $\phi_1-\phi_4$ ）的一个时钟触发的环计数器。一个块开始信号也连接到这个状态产生器的一个输入，并且被用于将这个环计数器保持在一个预定状态，直到开始进行实际的消息信息解码。当这个块开始信号释放这个状态产生器时，这个状态产生器开始产生与输入消息符号同步的、时钟触发的状态信号。

然后，这个时钟触发的状态信号各输出连接到一个状态选择器 828 的各输入。在工作期间，这个控制器 816 从这个码存储器 822 中恢复金融消息单元被分配的传送状态号码。这个状态号码被传送到这个控制器 816 的状态选择输出（ ϕ 选择），并且连接到状态选择器 828 的一

个输入。与被分配的发送状态相应的一个状态时钟被提供在状态选择器 828 的输出，并且分别连接到解复用器 820、块去交织器 824、地址和数据解码器 830 和 832 的时钟输入。解复用器 820 用于选择与被分配的发送状态相关的二进制比特，然后，这些二进制比特连接到块去交织器 824 的输入，并且在每一个相应的状态时钟下，被时钟信号输入到去交织器阵列中。在一第一实施方式中，这个去交织器使用一个 8×32 比特阵列，它去交织与一个发送信息块相应的、8 个 32 比特的交织地址、控制或者消息码字。被去交织的地址码字连接到地址相关器 830 的输入。这个控制器 816 恢复分配到金融消息单元的地址图形，并且将这个图形连接到这个地址相关器的一第二输入。当任何一个去交织的地址码字在一个可接受的错误限度内（例如，根据所选择的码字结构，可纠正的比特错误数目）与被分配到这个金融消息单元的任何一个地址图形匹配时，这个消息信息和与这个地址相关的相应信息（例如，表示被广播的和被接收的选择性呼叫信令消息，前面被定义为与消息相关的信息）然后被这个数据解码器 832 进行解码，并且被保存在一个消息存储器 850 中。

在检测到与金融消息单元相关的一个地址后，这个消息信息连接到数据解码器 832 的输入，数据解码器 832 将被编码的消息信息优选解码为适合于保存和随后显示的一个 BCD 或者 ASCII 格式。

替代地，基于软件的信号处理器可以被一个等效的硬件信号处理器替代，这个信号处理器用于恢复被分配到金融消息单元的地址图形和与消息相关的信息。在检测到与金融消息单元相关的一个地址后，或者在检测到与金融消息单元相关的一个地址前，这个消息信息和与这个地址相关的相应信息可以被直接保存在消息存储器 850 中。以这样的方式进行工作，就可以允许后面对实际消息信息的解码，例如，将被编码的消息信息解码成适合于随后进行显示的一个 BCD, ASCII, 或者多媒体格式。但是，在执行直接保存的过程中，这个存储器必须以这样的方式来构造，即能够有效地、高速地放置消息信息和与这个地址相关的相应信息。另外，为了方便实现将消息信息和与这个地址

相关的相应信息直接保存在消息存储器 850 中，一个码字标识器 852 检查所接收的码字来将一个类型标识分配到这个码字，以对属于包括一个矢量字段的一个集合和包括一个消息字段的一个集合中的一个集合的码字作出响应。在决定了类型标识后，一个存储器控制器 854 进行工作，来将这个类型标识保存在与这个码字相应的存储器内的一第二存储器区域中。在下面的专利中，更充分地讨论包括消息存储器 850、码字标识器 852 和存储器控制器 854 的去交织信息存储器保存装置的上述结构和操作。

在保存与消息相关的信息后，这个控制器 816 产生一个可感知的提示信号。优选地，这个可感知的提示信号是一个可听的提示信号，但是应理解，也可以产生其它可感知的提示信号，例如可触摸的提示信号，和可看的提示信号。这个可听的提示信号被这个控制器 816 连接到一个提示驱动器 834，这个提示驱动器 834 用于驱动一个可听的提示装置，例如一个扬声器或者一个换能器 836。这个用户可以使用一个该领域内众所周知的方式，通过使用用户输入控制 838 来取消提示信号的产生。

这个用户可以使用用户输入控制 838 来检索被保存的消息信息，其中，这个控制器 816 从存储器恢复这个消息信息，并且将这个消息信息提供到一个显示驱动器 840，以显示在一个显示器 842 上，例如一个 LCD 显示器上。

除了前面的描述，通过参考下述美国专利：Nelson 等等所发表的、题为“时分复用选择性呼叫系统”，专利号为 No.5, 168, 493, Nelson 等等所发表的、题为“用于接收一个多状态复用信号的选择性呼叫接收器”，专利号为 No.5, 371, 737, DeLuca 等等所发表的、题为“选择性呼叫信令系统”，专利号为 No.5, 128, 665, 和 Willard 等等所发表的、题为“同步选择性信令系统”，专利号为 No.5, 325, 088，所有这些专利的受让人是 Motorola 公司，并且其思想在这里被用作参考。

参考图 9，一个图显示了根据本发明的一个安全消息系统 900。

这个寻呼终端 102，或者无线选择性呼叫信令系统控制器，接收包含包括一个目的标识和一个安全金融交易消息的一个选择性呼叫消息请求的信息。典型地，这个信息经过一个公共交换电话网（PSTN）912 连接到这个寻呼终端 102，PSTN912 用于从一个调控者 914，例如一个银行、一个信用卡发行商或者类似的机构，发送这个信息。这个 PSTN912 可以使用传统的电话线 910，或者可能是一个高速的数字网络，连接到这个寻呼终端 102 和这个调控者 914，这与在这个调控者 914 和多个金融消息单元 906 之间交换金融交易所需要的信息带宽有关。一旦连接到这个寻呼终端 102，这个信息就被格式化为一个或者多个选择性呼叫消息，并且被传送到 922 至少一个无线频率发送器 904，以广播到位于多个通信区域 902 中任何一个通信区域中的至少一个金融消息单元 906。这个金融消息单元 906 可能包括一个接口，以将没有加密的或者加密的信息例如安全金融交易消息连接到一个传统的智能卡 920，进行一个金融交易。替代地，当这个金融消息单元 906 包括例如载入现金卡和重新载入和/或者信用卡服务能力，例如一个智能卡 920 中的能力时，这个安全金融交易消息可以被金融消息单元 906 解码和保存。

使用一个有线的或者一个无线的返回路径，可以为金融消息单元 906 提供一个双向的能力。作为示例，这个金融消息单元 906 接收这个安全的金融交易消息，并且解码和解密可能表示一个现金值令牌，信用或者借记数量的安全金融交易消息的内容。然后，这个消息内容被金融消息单元 906 所保存，金融消息单元 906 挂起对接收的证实和随后调控者所进行的资金释放或者信用卡授权。如果金融交易值高，在激活基于所接收的令牌资金以前，或者在允许一个信用卡或者借记交易以前，这个调控者典型地需要金融消息单元 906 发送来的一个确认。但是，如果金融交易值低，在激活基于所接收的令牌资金以前，或者在允许一个信用或者借记交易以前，这个调控者不需要金融消息单元 906 发送来的一个确认。在一个交易额低的交易情形下，金融消息单元 906 可能仅需要一天一次，或者一周一次地来保持其资金或者

信用卡能力一致。

图 9 所显示的这个安全消息系统允许使用分布式接收器站点 908 所接收的一个反向的或者向内的信道，使用无线的方式返回或者发起安全金融交易消息。典型地，这些站点比向外的广播站点 904 密集得多，这是因为金融消息单元 906 的发送器功率和天线特性比一个专用无线频率基站和广域发送器站点 904 的发送器功率和天线特性差得多。这样，一个金融消息单元 906 的尺寸和重量保持最小，实现了一个更人体工程的、便携式装置，并且具有不需要一个物理连接就实现金融交易，例如银行取钱，存款，信用卡支付，或者购买交易等的增值服务。替代地，这个安全消息系统被调节成容纳可能包括用于实现返回和发起安全金融交易消息的附加装置的、功率消耗较少的金融消息单元 906，安全金融交易消息的返回和发起使用在销售点 916 或者在一个银行 914 可以访问的一个反向或者向内信道来实现。在这些情形下，这个功率消耗较少的金融消息单元 906 包括一个红外或者激光端口，功率消耗较少的邻近磁感应或者电容端口，或者可能是一个超声或者音频带的声学换能器端口，所有这些端口均可以在功率消耗较少的金融消息单元 906 和一个装置，例如一个销售点处的终端、自动柜员机等，之间进行信号的连接。

几种密码方法适合于用于本发明。在理解与应用到有线或者无线通信的密码术相关的术语时，下述定义是有用的。

证书 - 证书是证明一个公钥与一个个体或者其它实体之间的绑定的数字文档。证书是由一个证书管理机构（CA）颁发的，这个证书管理机构可以是任何可以信赖的、愿意担保它向他们颁发证书的那些实体的身份的中心管理机构。当一个 CA 签发了一个用户的公钥加上其它标识信息，将这个用户与他们的公钥绑定 在一起时，就产生了一个证书。用户将他们的证书提供给其它用户，以表明他们公钥的真实性。

机密性 - 使信息对除被授权看它的人以外的所有其它人均是秘密的结果。机密性也称作保密性。

密码协议 - 一个分布式算法，由一系列精确定规定两个或者多个实

体所需要采取的动作来实现一个特定的安全目的的步骤所定义。

数据完整性 - 确保信息没有被任何没有授权的装置或者任何不知道的装置所更改。

解密 - 将被加密的信息（加密文本）转换为明文的过程。

DES（**数据加密标准**） - 一个对称加密算法，由美国政府所定义并且已经被美国政府确认为一个政府标准。它是世界上最有名的并且被广泛使用的密码系统。

diffie-Hellman - **Diffie-Hellman** 密钥约定协议，通过允许实体安全地通过一个公开信道建立一个共享的保密密钥，第一次实际地解决了密钥分发的问题。这个安全性是基于离散对数问题。

数字签名 - 将一个消息（数字形式）与发起方联系在一起的一个数据串。这个密码原语用于提供认证性，数据完整性和不可抵赖性。

离散对数问题 - 要求寻找公式 $y=g^x \bmod p$ 中的指数 x 。这个离散对数问题被认为是困难的，并且是一个单向函数的强方向。

椭圆曲线密码系统（ECC） - 一个基于椭圆曲线上的离散对数问题的公钥密码系统。ECC 提供了任何公钥系统中最高的每比特强度，与其它系统相比，允许使用小得多的公钥。

加密 - 为了机密性或者保密性，将明文转换成密文的过程。

实体认证 - 确认一个实体（例如，一个人，金融消息单元，计算机终端，智能卡 920 等等）的身份。

因子分解 - 将一个整数分解为一个小整数集合，当将这些小整数相乘时又可以形成原整数的动作。RSA 基于大质数的因子分解。

信息安全功能 - 提供信息安全服务的加密和数字签名的处理。也称作安全原语。

信息安全服务 - 利用信息安全功能的目的。服务包括保密性或者机密性，认证，数据完整性和不可抵赖性。

密钥 - 一个数据串的形式，可以被信息安全功能所使用来执行密码计算的一个值。

密钥约定 - 一个密钥建立的方法，其中，作为两方或者更多方中

的每一个所提供或者进行相关的一个功能或者信息，从这两方或者更多方推导出一个共享密钥，以使没有任何一方能够预知所产生值。

密钥建立 - 任何可使二方或更多方得到共享保密密钥的过程，以用于随后的密码使用。

密钥管理 - 支持密钥建立和维护各方之间的在用密钥关系的处理和机制的集合。

密钥对 - 在一个公钥密码系统中，一个用户或者实体的公钥和私钥。一个密钥对中的密钥在数学上通过一个强单向函数相关。

密钥传送 - 一个密钥的建立方法，其中一方产生或者另外获得一个秘密值，并且安全地将这个秘密值传送到其它方或者其它多方。

消息认证 - 确认信息源；也称作数据源的认证。

消息认证码（MAC） - 一个包括一个密钥，并且提供数据源认证和数据完整性的散列函数。这个 MAC 也称作一个交易认证码，其中一个消息可以包括至少一个交易。

不可抵赖性 - 避免对前面所进行的承诺委托或者动作进行否认。使用数字签名可以达到不可抵赖性。

私钥 - 在一个公钥系统中，它是一个密钥对中被个人用户所持有的、并且决不公开的密钥。最好将这个私钥嵌入在一个硬件平台中，作为其它未授权方不能够获得它的一个方法。

公钥 - 在一个公钥系统中，它是一个密钥对中可以公开的密钥。

公钥密码术 - 使用不同的密钥来进行加密（e）和解密（d）的一个密码系统，其中（e）和（d）在数学上是有联系的。不可能通过对（e）进行计算来决定出（d）。所以，这个系统允许分发公钥，而将私钥保持秘密。公钥密码术是在 2000 年后几年中，密码领域内最重要的改进。

RSA - 一个广泛使用的公钥加密系统，它是以其发明者 R. Rivest, A. Shamir, 和 L. Adleman 命名的。RSA 的安全性是基于整数因子分解问题的难处理性。

对称密钥加密 - 一个加密系统，其中对每一个相关的加密/解密密

钥对 (e, d) , 可以通过计算, 在仅知道 e 时很容易地决定 d , 或者从 d 决定 e 。在大多数实际的对称密钥解密方法中, $e=d$ 。尽管对称系统在对大量数据进行加密时的效率高, 但是它们产生了很重要的密钥管理问题。所以, 在一个系统中, 经常混合使用对称密钥和公钥系统, 以利用每一个的优点。

不对称密钥加密 - 一个加密系统, 其中对每一方来说, 可以持有长度可变的加密/解密密钥对, 例如, 在需要较少的安全性的情形下, 可使用长度较短的密钥, 而在需要更高的安全性的情形下, 可使用较长的密钥。如对称密钥加密系统一样, 不对称系统产生了重要的密钥管理问题。

证实-证实数字签名的过程, 由此认证了一个实体或者一个消息。

下述的示例显示了可以实现根据本发明的一个安全消息系统的系统。

使用 ECC 算法, 根据下述信息产生带散列的一个安全签名:

P 是曲线上的一个产生点, 并且其序号是 n 。

H 是一个安全的散列算法, 例如 SHA - 1。

M 是将要被一个实体 A 所签名的一个比特串。

A 有一个私钥 a 和一个公钥 $Y_a = aP$ 。

为了产生这个签名, 实体 A 进行下述计算:

1. 计算 $e=H(M)$ (e 是一个整数)。

2. 产生一个随机整数 k 。

3. 计算 $R = kP = (x, y)$

4. 将 x 转换为一个整数。

5. 计算 $r=x+e \bmod n$

6. 计算 $s=k-a r \bmod n$

7. 这个签名是 (r, s) 。

因为 $R = kP$ 的计算与消息 M 独立, 所以可以在对 M 签名以前预

计算，对 M 签名是在步骤（5）和（6）中进行的。在这个过程中，与其它被执行的操作相比，进行散列计算和产生一个随机数所需要的计算时间认为是可以被忽略的。最后，某些函数的预计算可以加快步骤（3）中 kP 的计算。

任何实体 B 可以通过执行下述步骤来证实 A 对 M 的签名 (r, s) :

1. 获得 A 的公钥 $Y_a = aP$ 。
2. 计算 $u = sP$ 。
3. 计算 $v = rY_a$
4. 计算 $u + v = (x', y')$ 。
5. 将 x' 转换为一个整数
6. 计算 $e' = r - x' \bmod n$
7. 计算 $e = H(M)$ 并且证实 $e' = e$ 。

下述示例显示了使用一个椭圆曲线加密方法的加密。假设实体 A 有一个私钥 a 和公钥 $Y_a = aP$ ，其中 P 是一个产生点。实体 B 使用下述过程来加密将要传送到实体 A 的比特串 M :

1. B 获得 A 的公钥 Y_a
2. B 产生随机整数 k 。
3. B 计算 $R = kP$ 。
4. B 计算 $S = kY_a = (x, y)$
5. B 计算 $c_i = m_i \bullet f_i(x)$ 。
6. B 将 (R, c_0, \dots, c_n) 发送到 A。

其中 $f_0(x) = \text{SHA-1}(x || 0)$ 和 $f_i(x) = \text{SHA-1}(f_{i-1}(x) || x || i)$

替代地，如果 RSA 密码术被使用了，下述定义就是相关的：

n 是模数

d 是私钥和实体 A 的公用指数。

M 是需要被签名的一个比特串。

一个 RSA 签名被实体 A 按照如下的方式来产生：

1. 计算 $m = H(M)$ ，一个比 n 小的整数。

2. 计算 $s = m^d \bmod n$

3. 这个签名是 s.

如上所描述的 RSA 签名产生了带附录的数字签名。与前面讨论的 ECC 签名相比，当使用 RSA 时不需要进行预算算。注意，这个签名需要专用指数 d 的一个指数项。

实体 B 使用下述过程来证实 A 对 M 的签名 S:

1. 获得 A 的公用指数 e 和模数 n.

2. 计算 $m^* = s^e \bmod n$

3. 计算 $m = H(M)$.

4. 证实 $m^* = m$.

在 RSA 证实中，需要公用指数 e 的一个指数项。e 优选被选择为 64 比特随机数。类似地，对于 RSA 加密，需要带一个公用指数的指数项，并且为了具有最小的安全性，公用的指数需要至少为 64 位。

考虑到前面的讨论，参考图 10-16 来描述这个安全消息系统的余下部分。

参考图 10，图显示了根据本发明的优选实施方式的一个金融消息单元 906 的一个高级框图。

一个金融消息单元 906 的一个可能的实施方式是如图 10 所显示的一个传统的寻呼装置和智能卡 920 的组合。这里，一个机械的插槽和标准的智能卡连接器被容纳在这个寻呼装置的机壳内，以使一个智能卡 920 可以插入到这个机壳内从而在这个卡和寻呼器电子电路之间建立连接。替代地，需要实现一个智能卡 920 的电子电路被移到或者集成到这个寻呼装置中，这样，这个寻呼器就可以用作一个真正的无线智能卡或者无线 ATM。

在工作中，这个输入信号被连接到接收器 804 的天线 802 所捕获，接收器 804 检测和解调这个信号，并且恢复如前面参考图 8 所讨论的任何信息。替代地，这个金融消息单元 906 包含一个低功率反向信道发送器 1034，功率开关 1032，和发送天线 1030 以对一个向外信道查询作出响应或者产生一个向内信道请求。不用低功率无线频率发送器

1034 和其相关的部件，替代的发送模块 1036 可以包括单向或者双向通信换能器。这种换能器的示例有象激光器或者发光二极管（LED）的光学装置，极低功率的磁场感应或者电场电容结构（例如，线圈，传输线），或者可能是工作在音频或者超声波范围内的声波换能器。

一个输入/输出（I/O）开关 1002 用于在 RF 接收器 804, RF 发送器 1030 和一个选择性呼叫解码器 1004 之间引导输入 或者向外发送的无线频率（RF）能量。这个选择性呼叫解码器 1004 包括一个处理单元 1006, 和其相关的随机访问存储器(RAM)1008, 只读存储器(ROM)1010, 和通用输入/输出(I/O)模块 1012。这个选择性呼叫解码器 1004 的基本功能是检测和解码包括在要被这个金融消息单元 906 所接收的信令中的信息。替代地，在包括可选的反向信道发送器模块 1036 的一个双向实施方式中，这个选择性呼叫解码器 1004 也可以用作产生并且向调控者 914、一个用户或者其它在线系统（没有显示）发送请求或者消息的一个编码器。

另外，这个金融消息单元 906 包括一个安全的解码或者智能卡功能模块 1014。这个模块包括控制逻辑 1016, 一个消息输入装置 1018, 一个安全的码处理器 1020, 一个安全的 ROM1022, 一个安全的可编程只读存储器(PROM)1024, 和一个智能卡输入/输出(I/O)模块 1026.

特定的金融组已经提出了影响陆地有线环境中端到端交易安全性的标准。这些已提出的、用于进行安全的电子金融交易的标准是基于一个对等体到对等体的闭环系统，在这个闭环系统中，这个发送方（例如，一个调控者，或者发送者，例如一个银行，或者 VISATM）产生包括一个值数量和一个认证代码的一个安全交易。这个安全交易经过一个装置，例如一个自动柜员取款机（ATM）被传送到一个请求方。为了建立和完成一个交易，这个请求方将一个智能卡 920 插入到 ATM 中，输入一个识别代码，并且请求将一个值放置到这个智能卡 920 中。这个交易处理系统对这个智能卡 920, 这个请求方的金融状况（例如，帐户余额，可用的信用，等等）进行认证，并且或者完成或者否决这个交易。

所以，考虑到上述需求，这个控制逻辑 1016 进行工作来控制与这个智能卡功能模块 1014 相关的部件的工作，以在一个安全的金融交易消息中实现和维持端到端的安全性。这个控制逻辑 1016 确保任何与这个安全金融交易消息相关的内容被保持在一个对一个调控者 914 是加密的状态，直到它们被这个智能卡功能模块 1014 或者一个相关的智能卡 920 所实际解密。所以，敏感信息，例如一个私用加密密钥，现金载入值，信用卡或者银行帐户号码，或者类似的信息，被保存在安全的 PROM1024 中。类似地，这个安全的 ROM1022 可以保存用于对在这个智能卡功能模块 1014 和一个调控者 914、商人 916、或者另一个智能卡 920 之间交换的信息进行解密和加密的处理例程。

这个消息输入装置 1018 允许一个用户发起一个现金载入请求，现金交易，信用卡交易等。典型地，一个用户可以使用一个键盘，一个语音激发的识别装置，一个触摸装置（例如，屏幕或者触摸垫），或者其它方便的数据输入装置来输入一个请求。本发明中，一个用户可以请求将要与金融消息单元 906 进行交换的、基于交易的信息保存在这个金融消息单元 906 中以在后面可以传送到这个智能卡 920 中，或者请求直接传送到这个智能卡 920。使用这种方式，这个金融消息单元 906 像一个便携式自动柜员取款机一样地在工作，允许一个用户进行金融交易，而不需要实际访问一个物理的 ATM 机。

在金融消息单元 906 作为具有发起能力的便携式 ATM，智能卡功能模块 1014 作为与金融消息单元相耦合的一个第二安全消息发生器，与安全消息发生器相耦合的便携式发送器 1034 用于向选择性呼叫消息处理器 1104 广播金融交易请求。与选择性呼叫消息处理器 1104 相耦合的接收机 1204 用于接收金融交易请求并送至选择性呼叫消息处理器 1104。以此方式，金融消息单元 906 无需查询与陆线硬连网或 PSTN 的物理连接而进行金融交易。

对于在此讨论的无线电频率使能反向信道金融消息单元 906 的实现，本发明最好使用 Motorola ReFlex™ 双向无线寻呼系统基础设施和在以下文献中详细描述的协议：由 Simpson 等人于 1993 年 10 月 4

日提交的题为“用于识别无线通信系统中发射机的方法和设备”的美国 08/131,243 号专利申请；由 Ayerst 等人于 1995 年 3 月 3 日提交的题为“用于优化无线通信系统中接收机同步的方法和设备”的美国 08/398,274 号专利申请；于 1996 年 5 月 28 日授与 Ayerst 等人的题为“用于在固定系统接收机方改进消息接收的方法和设备”的美国专利 5,521,926；由 Ayerst 等人于 1995 年 7 月 5 日提交的题为“允许反向信道 Aloha 发送的正向信道协议”的美国 08/498,212 专利申请；以及 Wang 等人于 1995 年 7 月 14 日提交的题为“在双向消息网络中分配频率信道的系统和方法”的美国 08/502,399 专利申请，以上发明都转让给本发明的受让人，在此引用作为参考。

可以看到在诸如蜂窝和无线分组数据系统等其它双向信道系统中可以实现本发明。

特定的金融组已经提出了影响陆地有线环境中端到端交易安全性的标准。这些已提出的、用于进行安全的电子金融交易的标准是基于一个对等体到对等体的闭环系统，在这个闭环系统中，这个发送方（例如，一个调控者，或者发送者，例如一个银行，或者 VISATM）产生包括一个值数量和一个认证代码的一个安全交易。这个安全交易经过一个装置，例如一个自动柜员取款机（ATM）被传送到一个请求方。为了建立和完成一个交易，这个请求方将一个智能卡 920 插入到 ATM 中，输入一个识别代码，并且请求将一个值放置到这个智能卡 920 中。这个交易处理系统对这个智能卡 920，这个请求方的金融状况（例如，帐户余额，可用的信用，等等）进认证，并且或者完成或者否决这个交易。

在一个更宽的应用中，这个金融消息单元 906 可以被调节成进行通信，这样敏感的消息或者数据，以及电子资金传送信息可以经过一个寻呼信道或者类似的信道，被安全地传送到所希望的接收装置。

参考图 11，这个框图显示了可以被用于一个金融组织的前端设备上、来经过一个寻呼信道或者类似的信道将安全的电子资金转移授权发送到金融消息单元的消息组合和加密设备。

特别地，直接分支和客户呼叫被第一金融交易处理器 1100 所接收，这个第一金融交易处理器 1100 包括一个交易处理计算机 1102，一个用作一个安全消息产生器和安全消息解码器的一个消息处理和加密计算机 1104 或用作第一安全消息发生器、第一安全消息解码器以及选择呼叫消息分配器的选择呼叫消息处理器，它们都可用作选择呼叫消息处理器 1104，一个用户数据库 1106，和一个安全代码数据库 1108。这个交易处理计算机 1102 接收金融交易请求并且与这个消息处理和加密计算机 1104 进行通信，来根据包括在安全代码数据库 118 中、与这个请求者和这个交易类型相应的信息，产生和加密安全金融交易消息。这个消息处理和加密计算机 1104 也从被包括在这个用户数据库 1106 中的信息中决定一个目的标识，这允许这个消息处理和加密计算机 1104 能够将目的标识和其相应的安全金融交易消息传送到一个选择性呼叫发送服务 904 上。这个目的标识可能与一个传统的寻呼地址，一个蜂窝电话地址，或者任何唯一地标识与这个安全金融交易消息相关的一个目的地的其它地址相应。

图 11 中所显示的这个消息组合和加密设备将典型地被用于一个金融组织的前端设备上，以经过一个传统的寻呼信道或者类似的信道，将安全的电子资金转移授权发送到金融消息单元 906（例如，“无线 ATM”装置）。在下述的示例中，使用标准的金融计算机和数据结构来组合交易信息，并且分别使用被分配到目标装置和交易的公钥和私钥对这个消息进行加密。被分配到每一个装置的密钥，和它们的寻呼地址被保存在与处理计算机相关的用户数据库中。在对每一个消息进行加密后，它就被象一个普通的寻呼消息一样被经过这个公众电话系统发送到这个寻呼系统。

将参考图 12 更完全地讨论这个金融交易处理器 1100，这个金融交易处理器 1100 集成了这个第一金融交易处理器 1100 和一个无线选择性呼叫信令系统控制器。

参考图 12，图显示了一个无线选择性呼叫信令系统控制器的一个功能图，这个无线选择性呼叫信令系统控制器实现了能够与这个金融

消息单元交换信令的一个混合单向和双向安全消息系统。

这个无线选择性呼叫信令系统控制器 1200 包括这个第一金融交易处理器 1100 和一个发送器 104 及其相关的天线 904, 在一个双向的 RF 系统中, 还包括至少包括一个接收信号处理器和至少一个接收天线 908 的一个接收器 1202 系统。优选地, 至少一个接收器 1202 系统中的几个系统可以分布在一个很宽的地理区域, 来接收由双向金融消息单元 906 所广播的低功率发送。选择任何给定地区区域内的接收器 1202 系统的数目, 以确保所有传输得到足够复盖。该领域内的一个普通技术人员将理解, 这个数目是可变地, 并且明显地决定于地形, 建筑物, 植物, 和其它环境因素。

这个无线选择性呼叫信令系统控制器 1200 表示整个安全消息系统的一个闭耦合实现方式。实际上, 一个调控者 (例如一个银行, 信用卡发行商, 等等) 不希望具有维持 RF 网络基础设施, 即处理器 104 和相关的天线 904, 和这个至少一个接收器 1202 系统的责任。所以, 一个传统的无线消息服务提供者或者类似方, 将维护 RF 网络基础设施, 并且这个调控者将使用一个传统的方式来利用这个 RF 网络基础设施, 以在这个调控者和这个金融消息单元 906 之间交换安全的金融交易消息。

作为前一操作的第一替代, 这个选择性呼叫信令系统控制器 1200 可以进行工作来对从一个调控者接收的安全金融交易消息进行加密, 编码和发送等操作, 其中第一金融交易处理器 1100 已经产生并且对这个安全金融交易消息进行加密, 并且这个选择性呼叫信令系统控制器 1200 进一步对这个安全的金融交易消息进行第二次加密。通过使用一第二、不相关的加密来封装它, 增加了一个相关安全金融交易消息的安全性级别。随后, 这个金融消息单元 906 解码和解密这个进行了双加密的消息, 公开其加密状态下的安全金融交易消息, 并且从而维护一个金融交易所需要的端到端安全性。类似地, 这个选择性呼叫信令系统控制器 1200 接收从这个金融消息单元 906 所发起的消息, 并且将处于加密状态的这个安全金融交易消息传送到一个调控者, 以进行解

密和处理。

作为前一操作的一第二替代，这个选择性呼叫信令系统控制器 1200 可以进行工作，来对在这个调控者和这个金融消息单元 906 之间交换的安全金融交易消息进行编码和进行发送。在这个情形下，在调控者处的这个第一金融交易处理器 110 已经产生并且对这个安全金融交易消息进行加密，并且这个选择性呼叫信令系统控制器 1200 进行工作，根据一个接收的目的标识来将一个选择性呼叫地址与这个安全金融交易消息进行相关，然后发送一个所产生的选择性呼叫消息，以被这个金融消息单元 906 所接收。随后，这个金融消息单元 906 解码这个选择性呼叫消息，公开处于其加密状态下的这个安全金融交易消息，并且这样维护一个金融交易所需要的端到端安全性。就前面的操作来说，这个选择性呼叫信令系统控制器 1200 进一步进行工作，来接收从这个金融消息单元 906 发起的消息，并且将处于加密状态的这个安全金融交易消息传送到一个调控者，以进行解密和处理。

参考图 13，图使用与在电子工业领域内众所周知的国际标准组织（OSI）的格式类似的一个格式，显示了一个消息系统的各层。

就本发明来说，网络层 1302 是其上产生金融交易的一个点。然后，这些金融交易被传递到一个消息层 1304，在这个消息层 1304 中，形成合适的选择性呼叫消息以包括在一个传送协议，例如 MotorolaTM 的 FLEXTM 或者 POCSAG 中。信道信令层 1306 或者传送层表示实现上述低层传送协议的点。最后，RF 信道是低层传送协议在其上交换包括金融交易的这个选择性呼叫消息的物理媒质。

参考图 14，这个流图显示了根据本发明的优选实施方式，一个金融消息单元的典型操作。

当激发 1400 时，这个金融消息单元 906（为了进行清晰的解释，标识为一个寻呼机）“正常”工作，即它在一个待机状态中进行等待，以搜寻其选择性呼叫地址 1404。如果这个金融消息单元检测到其地址，并且特别地，它检测到一个安全性地址 1406，例如一个与一单个唯一帐户相关的或者几个唯一帐户中一个相关的一特定选择性呼叫地址，

这个金融消息单元 906 恢复这个安全的金融交易消息来实施一个金融交易。一旦这个金融消息单元 906 判断出已经接收到一个安全的金融交易消息，就激发 1408 这个智能卡功能模块 1014，并且解码 1410 这个安全的金融交易消息。这里，所描述的解码表示从原选择性呼叫协议，例如，从一个 FLEX™ 或者 POCSAG 数据或者信息词恢复这个安全的金融交易消息，或者解码包括对这个安全的金融交易消息进行解密来恢复表示一个电子现金记号值，一个信用卡值，一个借记值，或者其它涉及一个安全金融交易的信息例如加密消息或者会话密钥的内容的步骤。根据这个安全金融交易消息的内容，这个控制逻辑 1016 和处理器 1006 进行工作，来执行与正在被执行的金融交易相关的指令 1412。

参考图 15，图形显示了通过和从一个无线金融消息单元，与请求和对资金的电子转移或者资金的借记相关的一个典型序列。

一个客户呼叫他或者她的银行 1502 来激发一个金融转移序列，经过一个 PIN 号码或者其它帐户信息 1506 识别他们自己，并且经过与他们的无线金融消息单元 906 进行通信，来请求一个转移或者其它金融交易。

在证实这个客户 1510 的身份和证实这个合适的帐号信息 1512 后，这个银行或者调控者发起一个事件序列来实现资金的电子转移，确认信用等。在一第一情形下，当这个金融交易请求被认证为从一个授权方发起，并且这个金融交易被一个调控者 1514 所允许时，就同意一个金融交易。典型地，当一方的资金足够进行一个现金载入或者借记请求时，或者当一方有足够的信用来完成一个交易时，调控者就允许金融交易。优选地，在同意进行金融交易后，这个金融消息单元 906 提示这个用户等待这个交易 1520，并且这个系统开始完成这个金融交易 1522。

在一第二情形下，当其中至少一个金融交易请求被认证为不是从一个授权方发起的和这个金融交易不被一个调控者 1516 允许时，第一金融交易处理器就不同意完成根据这个金融交易请求的这个金融交

易。典型地，当一方在其现金载入中没有足够的资金时，或者当一方没有足够的信用来完成一个交易时，调控者就否决这个金融交易。如果这个调控者否决这个金融交易，这个请求被终结 1518，并且这个金融消息单元 906 返回到正常操作。

参考图 16，图形显示了通过和从一个单向和一个双向安全通信系统中的一个无线金融消息单元，与请求和对资金的无线转移或者资金的借记相关的一个典型序列。

通过这个调控者或者发行商搜寻与至少一个金融消息单元 906 相关的一个用户帐号 1602 的目的标识和安全代码（例如，公钥或者私钥），开始完成这个金融交易。然后，这个安全的消息系统产生将要被发送到这个无线选择性呼叫信令系统控制器的安全金融交易消息，在这个无线选择性呼叫信令系统控制器中，这个选择性呼叫消息处理器执行一个控制程序，来接收包括一个目的标识和安全金融交易消息的选择性呼叫消息请求，并且将这个安全金融交易消息封装 在包括与这个目的标识相应的一个选择性呼叫地址的一个选择性呼叫消息中。这个选择性呼叫消息然后被分发到一个选择性呼叫发送服务，以对这个目的标识作出响应。这个选择性呼叫发送服务将这个选择性呼叫消息广播到接收这个选择性呼叫消息的金融消息单元 906。可选地，这个金融消息单元 906 可能发送一第一消息来提示这个用户插入一个智能卡 920，来进行资金转移或者类似的交易。然后，这个银行等待 1606 一个合适的时间 1608，然后发送一个数据传输，这个数据包括带需要被信贷的智能卡 920 的帐号，这个交易的数量，和编码信息的信息，以证实这个需要被借记的智能卡 920 是合法的，并且不是一个仿制品 1610。很明显，如果这个智能卡 920 与这个金融消息单元 906 集成在一起，就不需要执行步骤 1604，1606，和 1608。典型地，一个银行将在一个交易完成 1614 后，记录 1612 这个交易的成功或者失败。

在具有双向能力 1616 的一个金融消息单元 906 中，这个银行等待接收包括证实金融交易执行的、一个返回的、安全的金融交易消息的一个确认 1618。当成功 地完成了这个金融交易时，在这个金融消息

单元 906 返回到一个空闲状态 1626 以前, 在这个金融消息单元 906 上, 一个可选的消息被提供 1624 给这个用户。替代地, 如果在一预定的延迟期间 1620 内, 没有接收到确认, 这个银行可能会重新发起前面的金融交易 1622。

在参考图 14-16 所讨论的操作的变化中, 这个用户可能在金融交易期间保持通信状态, 并且银行可能使用一个替代的路径, 即一个不是 RF 反向信道的路径, 接收关于这个交易被成功 完成的一个非实时的确认。可以通过使用在一个有线 ATM 机器中的单向或者双向寻呼装置, 或者在整个交易期间让这个用户保持使用一个电话或者其它通信装置, 来完成这一工作。另外, 这个金融消息单元 906 可以产生一个明显的音频提示样板, 来通知已经完成了这个金融交易而没有出现错误。

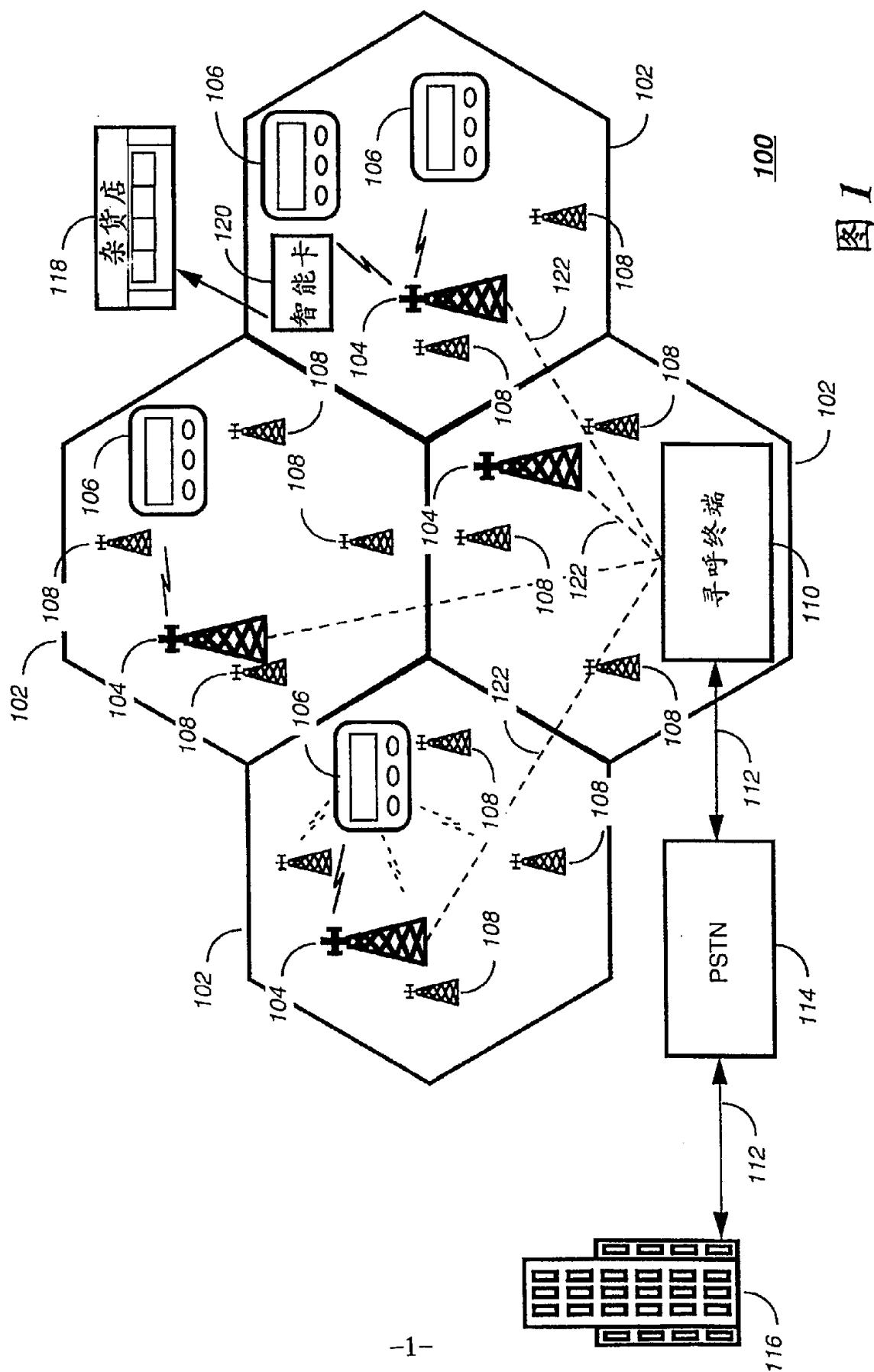
另外, 如果检测到与一个常规消息功能相关的一个地址, 这个金融消息单元 906 将用作一个常规的寻呼装置。但是, 如果被检测的地址与一个安全数据传输地址相关, 就激发这个安全的解码器模块, 并且可以对这个被接收的安全金融消息进行解密, 并且可以根据这个消息的内容或者根据与所接收的地址相关的规则来处理被包括在这个消息中的信息。

该领域的一个普通技术人员也可以理解, 与本发明相关的、前面所进行的讨论决不将这个系统局限于一个特定的传输协议, 无线媒质, 密码方式, 或者物理通信装置。所以, 本发明和根据这里的教义所可能进行的其它变化仅表示使用本发明的独特原理来实现用于交换金融信息的一个安全消息系统的一些有限的选择方法。

根据前面的精神, 我们将下述申请为我们的发明。

09.15

说 明 书 附 图



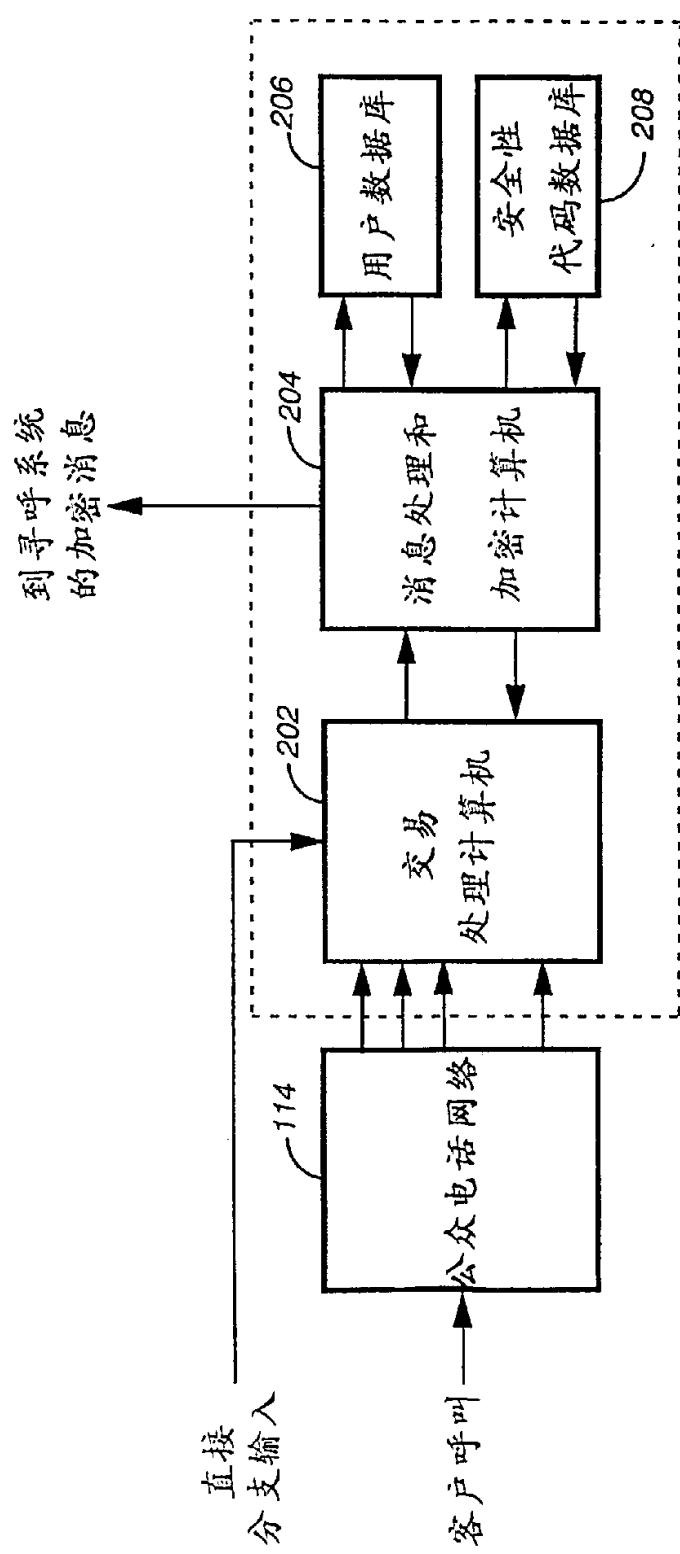


图2

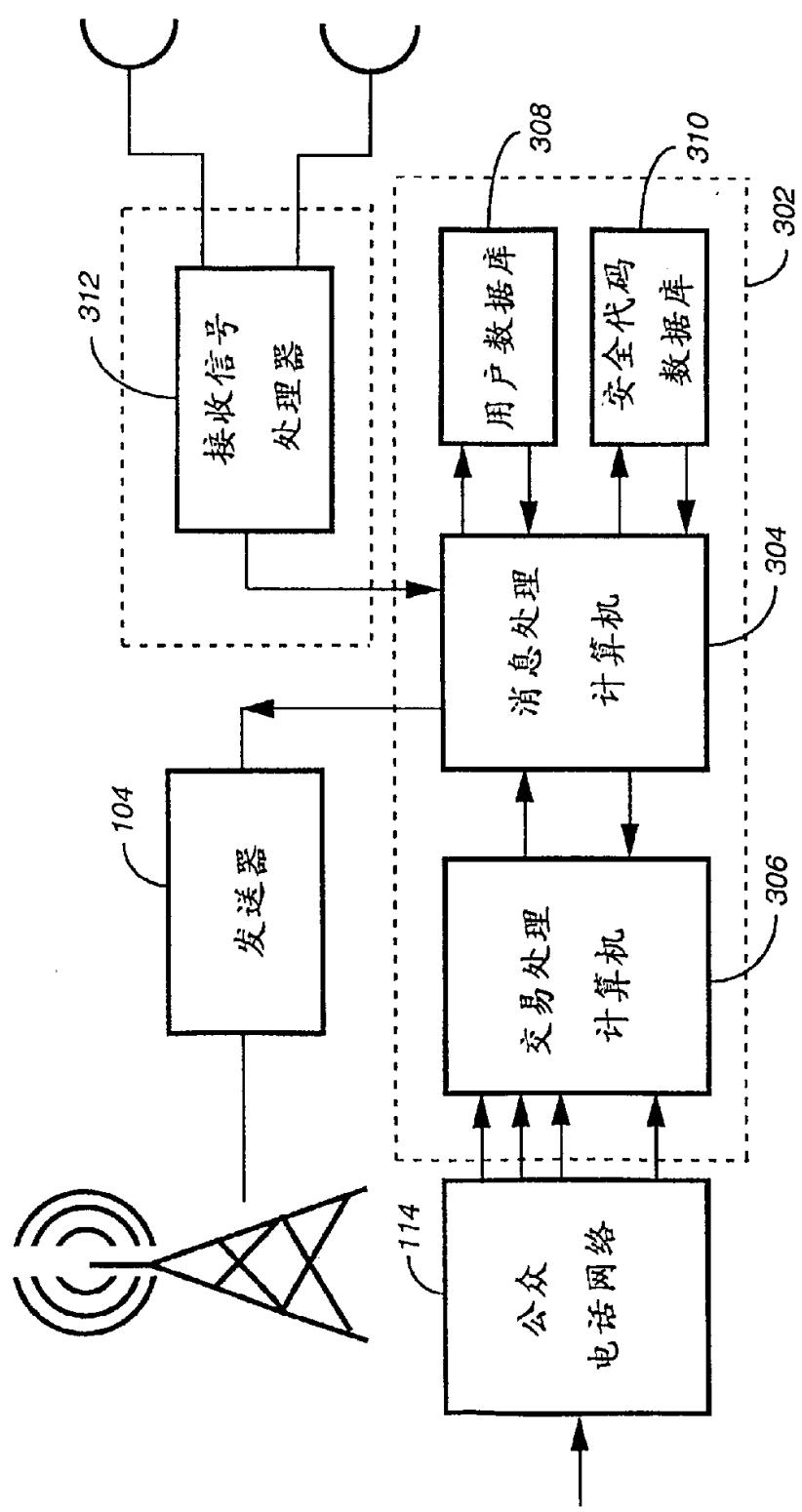
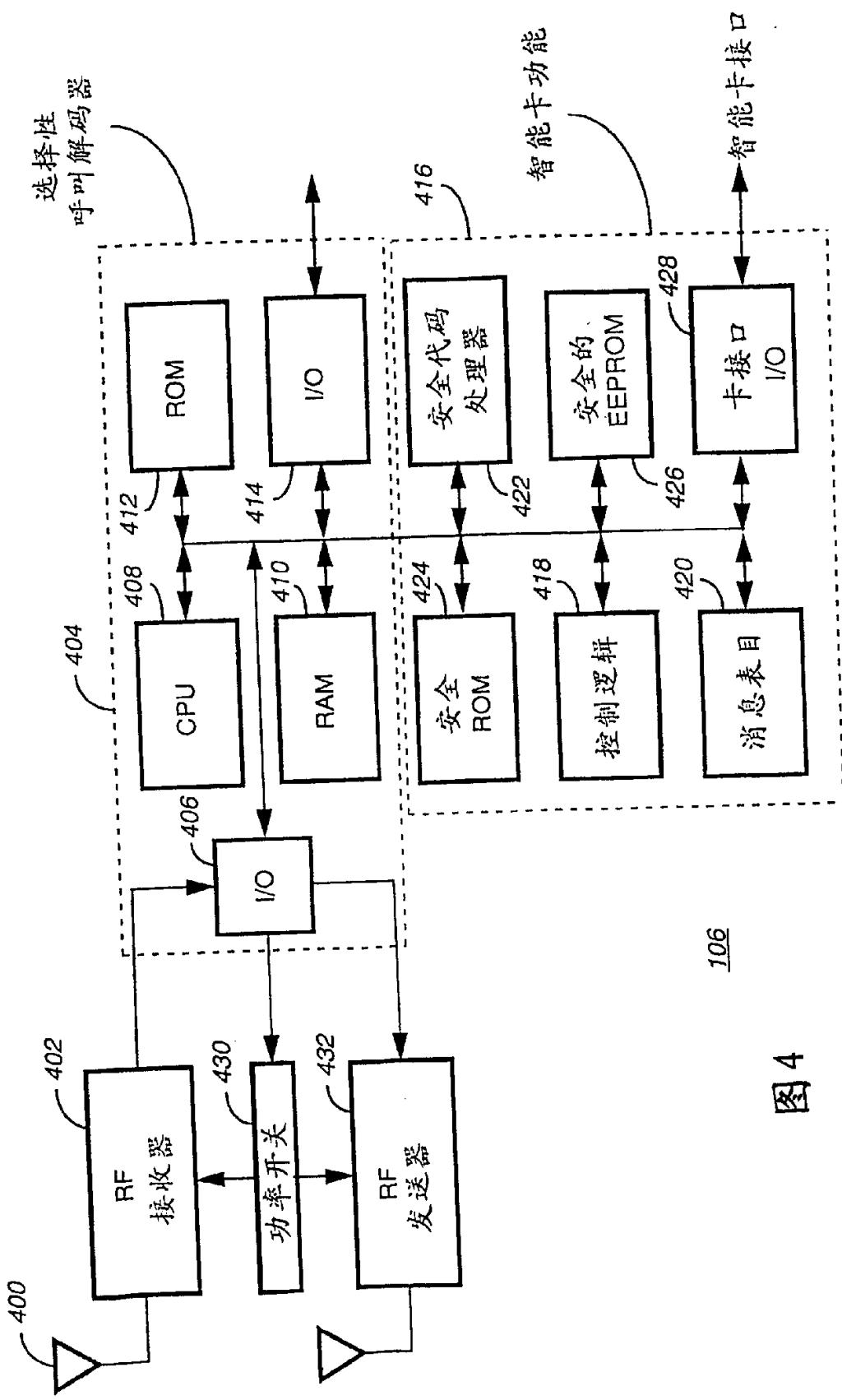


图3



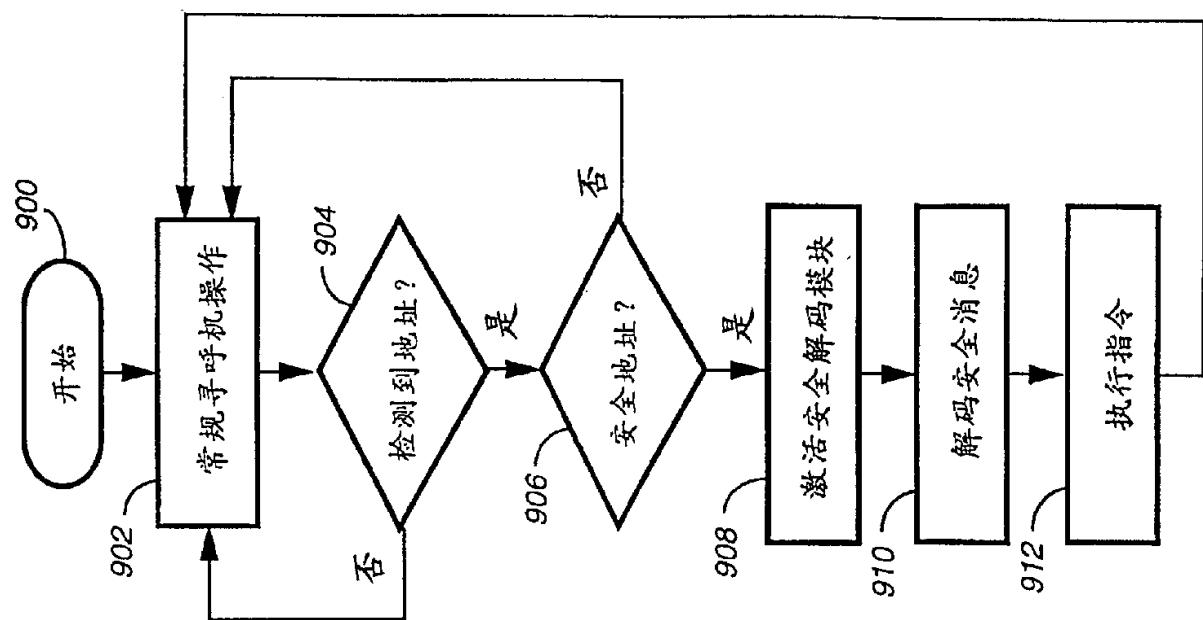


图9

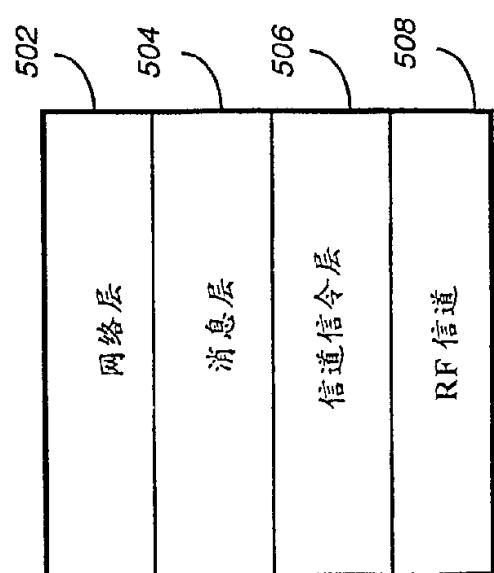


图5

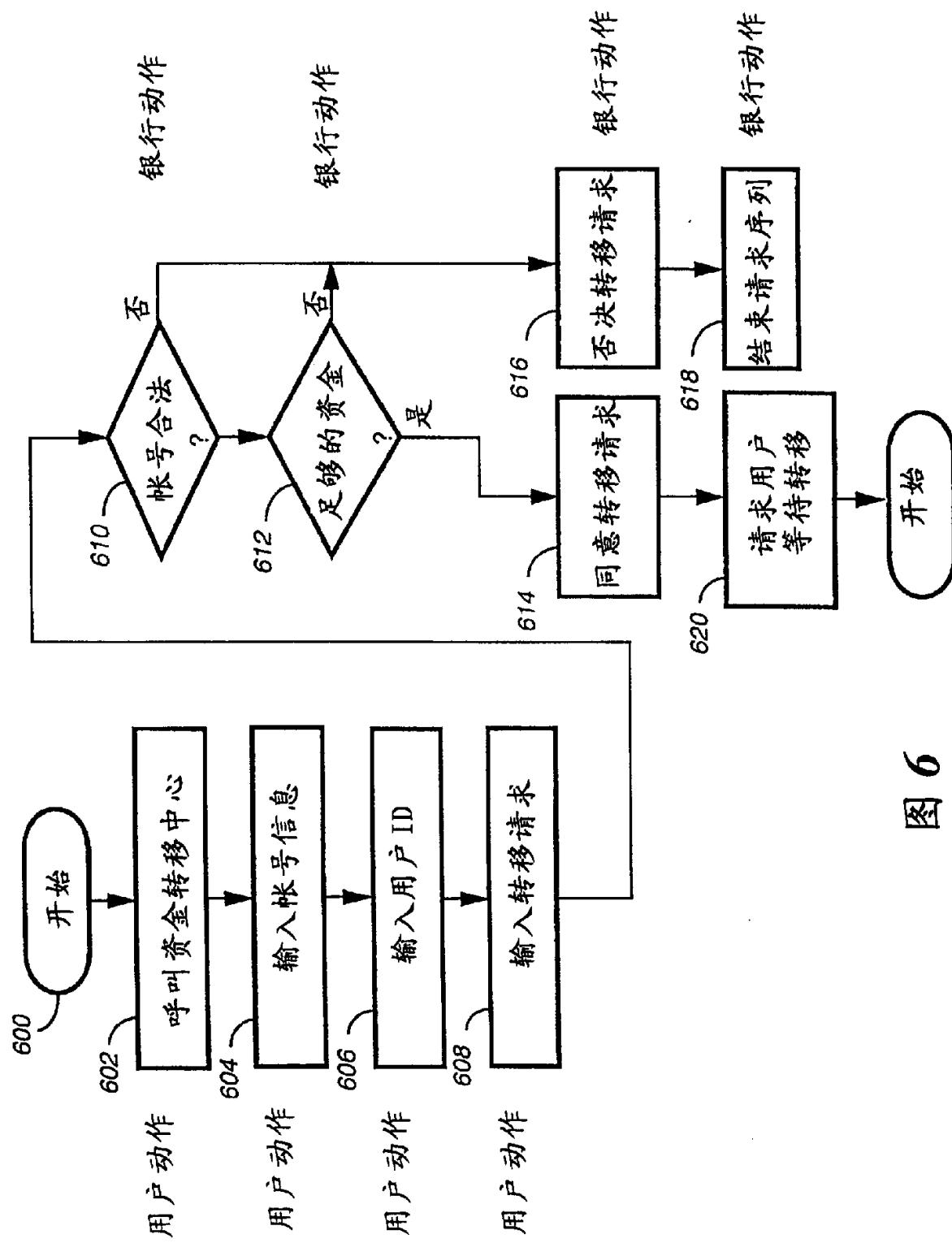


图 7

