(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 101960762 B
(45)授权公告日 2017.06.23

(21)申请号 200980107942.7

(22)申请日 2009.01.28

(65)同一申请的已公布的文献号
申请公布号 CN 101960762 A

(43)申请公布日 2011.01.26

(30)优先权数据
61/031,605 2008.02.26 US
61/031,885 2008.02.27 US
12/196,806 2008.08.22 US

(85)PCT国际申请进入国家阶段日
2010.09.06

(86)PCT国际申请的申请数据
PCT/US2009/032273 2009.01.28

(87)PCT国际申请的公布数据
WO2009/108444 EN 2009.09.03

(73)专利权人 巴特尔能源联合有限责任公司
地址 美国爱达荷州

(72)发明人 斯蒂文·H·麦考恩

(74)专利代理机构 北京律诚同业知识产权代理有限公司 11006
代理人 徐金国 谢雪闽

(51)Int.Cl.
G06Q 20/12(2012.01)
G06Q 20/22(2012.01)
G06Q 20/32(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)
G06Q 40/00(2012.01)
H04L 9/32(2006.01)

(56)对比文件
US 20070198432 A1,2007.08.23,
CN 1423472 A,2003.06.11,
CN 1516508 A,2004.07.28,

审查员 王侠

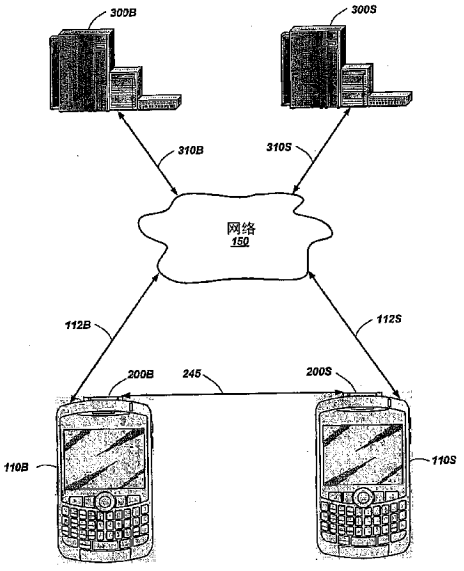
权利要求书2页 说明书13页 附图6页

(54)发明名称

用于执行无线金融交易的系统和方法

(57)摘要

一种安全计算模块(SCM)配置为与个人终端设备连接。该SCM包括:用于执行安全处理操作的处理器;用于将处理器耦合至个人终端设备的主机接口;和连接至处理器的存储器,其中该处理器逻辑地隔离至少一些存储器免于个人终端设备访问。该SCM还包括连接至处理器以与和另一个人终端设备关联的另一SCM进行通信的近场无线通信器。该SCM生成用于金融交易封包的安全数字签名,并使用近场无线通信器将该封包和签名传送给另一SCM。使用每个人的SCM的安全数字签名和可行的消息加密,在人与人之间执行金融交易。将数字签名和交易详情传送给适当的金融组织以验证交易方并完成该交易。



CN 101960762 B

1.一种可操作地耦合至个人终端设备的安全计算模块，其中所述个人终端设备被配置以用于执行与另一个人终端设备进行安全无线金融交易，所述安全计算模块包括：

用于执行安全处理操作的处理器；

用于将处理器可操作地耦合至个人终端设备的个人终端接口；

可操作地耦合至处理器的存储器，其中该处理器物理地隔离至少一些所述存储器以免个人终端设备访问；和

近场无线通信器，其可操作地耦合至处理器，并配置用于当在与所述另一个人终端设备关联的另一安全计算模块的近场范围内时，和所述另一安全计算模块通信；

其中该安全计算模块被配置为生成用于金融交易封包的安全数字签名，并使用近场无线通信器，将该金融交易封包和该安全数字签名传送给所述另一安全计算模块。

2.权利要求1的安全计算模块，其中该安全计算模块进一步配置为指示个人终端设备将金融交易封包和安全数字签名传送给与个人终端设备的用户关联的金融组织。

3.权利要求1的安全计算模块，其中该安全计算模块进一步配置为将安全数字签名添加给自所述另一安全计算模块接收的第二金融交易封包。

4.权利要求1的安全计算模块，其中所述安全数字签名包括使用秘密密钥在包括金融交易详情和交易号码标识符的消息上执行的安全散列函数。

5.权利要求1的安全计算模块，其中该安全计算模块进一步配置为与个人终端设备隔离地、并在通过近场无线通信器或个人终端设备进行通信之前对该金融交易封包、安全数字签名或其组合进行加密。

6.权利要求5的安全计算模块，其中使用安全计算模块以及与个人终端设备的用户关联的金融组织已知的秘密密钥，利用对称加密处理来执行该加密。

7.权利要求5的安全计算模块，其中使用与另一个人终端设备的另一用户关联的公用密钥，利用非对称加密处理来执行该加密。

8.权利要求5的安全计算模块，其中使用与金融组织关联的公用密钥，利用非对称加密处理来执行该加密。

9.权利要求1的安全计算模块，其中该安全计算模块进一步配置为对从所述另一安全计算模块接收的金融交易封包进行解密。

10.权利要求1的安全计算模块，其中所述近场无线通信器配置为使用可用的射频、红外频率、802.1a/b/g/n型无线连接、蓝牙、RFID、WiFi、WiMax或其组合进行通信。

11.权利要求1的安全计算模块，其中所述安全计算模块配置为与个人终端设备可拆除地耦合。

12.权利要求1的安全计算模块，其中所述安全计算模块可操作地集成在个人终端设备内。

13.权利要求1的安全计算模块，其中所述个人终端设备选自于包括下述的组中：蜂窝电话、智能电话、寻呼机、个人数字助理、手持式计算平台、腕戴式计算系统、移动计算系统和桌面计算系统。

14.一种用于在两个实体之间传送安全金融交易封包的系统，包括：

与买方关联的第一个人终端设备，其包括与其操作地耦合的第一安全计算模块，该第一安全计算模块配置为：

利用安全存储器的存储程序生成用于金融交易封包的买方的安全数字签名，其中所述安全存储器被物理地隔离以免被所述第一个人终端设备访问；和

当在第二安全计算模块的近场范围内时，将金融交易封包和买方的安全数字签名传送给所述第二安全计算模块；和

与卖方关联的第二个人终端设备，其包括与其操作地耦合的第二安全计算模块，该第二安全计算模块配置为：

生成用于金融交易封包的卖方的安全数字签名；和

当在第一安全计算模块的近场范围内时，将金融交易封包和卖方的安全数字签名传送给所述第一安全计算模块。

用于执行无线金融交易的系统和方法

[0001] 相关申请

[0002] 本专利申请要求于2008年8月22日提交的序列号为12/196,806,标题为“SYSTEM AND METHODS FOR PERFORMING WIRELESS FINANCIAL TRANSACTIONS”的美国非临时专利申请的利益和优先权,要求于2008年2月26日提交的序列号为61/031,605,标题为“PHONE-TO-PHONE FINANCIAL TRANSACTION SYSTEM”的美国临时专利申请的利益和优先权,要求于2008年2月27日提交的序列号为61/031,885,标题为“PHONE-TO-PHONE FILE DISTRIBUTION SYSTEM WITH PAYMENT”的美国临时专利申请的利益和优先权,在此将每个申请全文引入作为参考。

[0003] 本申请还涉及于2008年8月22日提交的序列号为12/196,669,代理人案件号BA-314,标题为“SYSTEM AND METHODS FOR PERFORMING FILE DISTRIBUTION AND PURCHASE”的美国非临时专利申请,和在同一天提交的代理人案件号BA-314PCT,标题为“SYSTEM AND METHODS FOR PERFORMING FILE DISTRIBUTION AND PURCHASE”的相应PCT申请。

[0004] 政府权利

[0005] 根据在美国能源部和Battelle Energy Alliance,LLC.之间的合同DE-AC07-05-ID14517,美国政府拥有本发明中的某些权利。

技术领域

[0006] 本发明的实施例一般地涉及无线通信系统,更具体地,涉及使用无线通信系统执行金融交易的系统和方法。

背景技术

[0007] 多年来,蜂窝电话主要设计用于提供无线语音通信。然而,随着技术的最新发展,已经将附加功能添加给蜂窝电话,有时将其称作个人无线设备。例如,包括蜂窝电话、个人数字助理、电子邮件客户端、媒体播放器和数字照相机功能的个人无线设备现在很普及。由于这些设备的增加性能,许多用户使用这些设备存储或访问敏感信息(例如金融账户信息)或者访问专用网络(例如公司网络)。

[0008] 就金融交易而言,安全和防止欺诈的创新对于新形式无线交易的市场拓展和用户接受性是至关重要的。例如,无论亲自执行还是在互联网上执行的信用卡交易都易受到经验逐渐丰富复杂的窃贼们的欺诈和窃取。这些攻击涉及偷取信用卡收据或者复制卡号以攻击网页可访问的数据库,从而获取大量的信用卡帐号。由于这些类型攻击的欺诈,每年因为这些初始资金偷窃以及导致的身份偷窃而导致数十亿美元的损失,。

[0009] 除了对于防止欺诈的努力之外,信用卡公司还不断寻找拓展他们的客户群的新方法。许多发展活动集中于征募可能需要建立信用的年轻人,例如那些首次进入市场的、具有获准花费的金钱的大学生和设法恢复不良信用的人。

[0010] 需要支持在个人之间的安全无线金融交易的系统和方法,其中个人可以安全地使用他们的无线设备结合他们的金融帐号来相互购买物品,而不需要固定的信用卡终端。

发明内容

[0011] 本发明的实施例包括在个人之间执行安全无线金融交易的系统和方法，其中个人可以安全地使用他们的无线设备结合他们的金融账户来相互购买物品，而不需要固定的信用卡终端。

[0012] 在本发明的一种实施例中，一种安全计算模块配置为可操作地耦合至个人终端设备。该安全计算模块包括：用于执行安全处理操作的处理器；用于将处理器可操作地耦合至个人终端设备的主机接口；和可操作地耦合至处理器的存储器，其中该处理器逻辑地隔离至少一些存储器以免个人终端设备访问。该安全计算模块还包括近场无线通信器，其可操作地耦合至处理器，并配置用于当处于另一安全计算模块的近场范围内，和与另一个人终端设备关联的另一安全计算模块进行通信。该安全计算模块配置为生成用于金融交易封包的安全数字签名，并使用近场无线通信器，将该金融交易封包和安全数字签名传送给所述另一安全计算模块。

[0013] 根据本发明的另一实施例，一种执行金融交易的方法包括：确定用于金融交易的金融交易详情，使用买方的安全数字签名对该金融交易详情进行签名，和使用卖方的安全数字签名对该金融交易详情进行签名。该金融交易详情、买方的安全数字签名和卖方的安全数字签名包括金融交易封包。通过近场无线通信信道，在买方无线通信设备和卖方无线通信设备之间传送该金融交易封包。该方法还包括：通过蜂窝通信信道，将该金融交易封包传送给卖方的金融组织；和将来自卖方金融组织的金融交易封包传送给买方的金融组织。卖方的金融组织验证卖方的安全数字签名和金融交易详情，和将卖方批准发送给买方的金融组织。买方的金融组织验证买方的安全数字签名和金融交易详情，将买方批准发送给卖方的金融组织，和执行从买方的金融组织到卖方的金融组织的资金转账。

[0014] 根据本发明的又一实施例，一种执行金融交易的方法包括：确定用于金融交易的金融交易详情，使用买方的安全数字签名对该金融交易详情进行签名，和使用卖方的安全数字签名对该金融交易详情进行签名。该金融交易详情、买方的安全数字签名和卖方的安全数字签名包括金融交易封包。通过近场无线通信信道在买方无线通信设备和卖方无线通信设备之间传送该金融交易封包。该方法还包括：通过蜂窝通信信道将该金融交易封包传送给买方的金融组织；和将来自买方金融组织的金融交易封包传送给卖方的金融组织。卖方的金融组织验证卖方的安全数字签名和金融交易详情，和将卖方批准发送给买方的金融组织。买方的金融组织验证买方的安全数字签名和金融交易详情，将买方批准发送给卖方的金融组织，和执行从买方的金融组织到卖方的金融组织的资金转账。

[0015] 根据本发明的又一实施例，一种执行金融交易的方法包括：确定用于金融交易的金融交易详情，使用买方安全数字签名对该金融交易详情进行签名，和使用卖方安全数字签名对该金融交易详情进行签名。该金融交易详情、买方安全数字签名和卖方安全数字签名包括金融交易封包。在买方的蜂窝通信设备和卖方的互联网站点之间传送该金融交易封包。该方法还包括将该金融交易封包传送给买方的金融组织和卖方的金融组织。卖方的金融组织验证卖方的安全数字签名和金融交易详情，和将卖方批准发送给买方的金融组织。买方的金融组织验证买方的安全数字签名和金融交易详情，将买方批准发送给卖方的金融组织，和执行从买方的金融组织到卖方的金融组织的资金转账。

附图说明

[0016] 图1图示包括个人终端设备和安全计算模块的通信系统；

[0017] 图2图示在适合于插入蜂窝通信设备的卡内实施的安全计算模块的前视图；

[0018] 图2A图示使用半透明视图图示图2的安全计算模块的等距视图，图示根据本发明实施例的内部组件；

[0019] 图3图示自蜂窝通信设备断开连接的安全计算模块；

[0020] 图3A图示物理和电连接至蜂窝通信设备的安全计算模块；

[0021] 图4图示与蜂窝通信设备通信的安全计算模块的简化方框图；

[0022] 图5图示用于执行在个人之间的金融交易的通信系统的简化系统图；和

[0023] 图6是图示在个人之间的金融交易期间可以执行的动作的简化流程图。

具体实施方式

[0024] 在随后的详细描述中，参考构成其一部分的附图，其中说明性地图示了可以实现本发明的具体实施例。足够详细地描述这些实施例以使本领域的普通技术人员能够实现本发明。然而，应当理解仅仅说明性地而非限制性地给出了详细描述和具体实例，同时指出本发明实施例的实例。根据公开内容，在本发明保护范围之内的各种替代、修改、添加、重新配置或其组合可以由本领域的技术人员实现，并将是显而易见的。

[0025] 本发明的实施例包括在个人之间执行安全无线金融交易的系统和方法，其中个人可以安全地使用他们的无线设备结合他们的金融账户来相互购买物品，而不需要固定的信用卡终端。

[0026] 该系统和方法包括电话对电话金融交易系统，其通过增设带有软件的个人电子设备(PED)和用于执行该软件的安全计算模块(SCM)，实现安全的个人对个人金融交易。该SCM可以是可嵌入或者已嵌入PED内的处理硬件。

[0027] 如在此使用的，PED可以是由用户使用的任意移动计算设备，并能够使用蜂窝无线通信信道进行通信。在此还可以将PED称作个人终端设备、蜂窝通信设备或无线通信设备。PED的实例包括蜂窝电话、智能电话、黑莓®智能电话、寻呼机、个人数字助理、音乐播放器(例如MP3播放器和Ipod)、手持式计算平台、腕戴式计算系统或其它移动计算系统(例如笔记本)。此外，该个人终端设备还可以是台式计算机或其它设备，例如装备有安全计算模块的卫星电视接收机、数字通用盘(DVD)播放器和视频卡带录像机(VCR)。

[0028] 图1图示包括个人终端设备110、服务器180、网络150、无线通信基站140和安全计算模块200的通信系统100。

[0029] 在一些实施例中，个人终端设备110可以是蜂窝通信设备110。蜂窝通信设备110可以使用可以是蜂窝无线信道的无线信道112与基站140通信。蜂窝通信设备110可以是无线通信设备，例如智能电话、黑莓®智能电话、笔记本计算机或配置为与陆地蜂窝基站140通信的其它适当设备。基站140可以与网络150通信。网络150可以是诸如互联网、公共交换电话网或用于实现通信的任何其它适当配置的通信网络。

[0030] 蜂窝通信设备110可以包括用于向用户传送信息的显示器和用于供用户向蜂窝通信设备110传送信息的键盘。

[0031] 安全计算模块200可以物理地连接至蜂窝通信设备110。作为非限制性的例子，可以将安全计算模块200配置为适合于插入个人终端设备110的卡。尽管物理地连接至个人终端设备110，但安全计算模块200可以独立地和/或与个人终端设备110隔离地执行软件。

[0032] 图2图示在适合于插入蜂窝通信设备110中的卡内嵌入的安全计算模块200的前视图。图2A使用半透明视图图示图2的安全计算模块200的等距视图，以图示根据本发明实施例的内部组件。该安全计算模块200可以具有类似于安全数字(SD)存储卡的物理特性。例如，该安全计算模块200可以包括尺寸基本上类似于SD存储卡的外壳204。此外，该安全计算模块200可以包括配置为物理地和电连接至蜂窝通信设备110的主机接口202。作为非限制性的例子，可以将该主机接口202配置为SD输入/输出(SDIO)接口、安全数字高容量(SDHC)接口或适合于插入蜂窝通信设备110的扩展槽的其它接口。如图2A所示，安全计算模块200可以包括外壳204、电路206和主机接口202。

[0033] 外壳204通过围绕电路206来容纳电路206，并可以允许用户操作安全计算模块200，而不破坏电路206，以便电路206并不物理地暴露给用户。

[0034] 如图2和2A所示，一些实施例可以配置为包括安全计算模块200的外壳204不同于个人终端设备110并可从其拆除。在其它实施例中，安全计算模块200可以不包括外壳，并可以内嵌在蜂窝通信设备110内。在任一实施例中，安全计算模块200配置为至少维持与蜂窝通信设备110的逻辑隔离，如下文中更完整地解释的。

[0035] 电路206可以包括一个或多个集成电路，并可以包括一个或多个电路板。电路206可以配置为执行安全计算模块200的功能。

[0036] 当然，安全计算模块200可以配置为具有除了SD外形因素之外的外形因素。例如，安全计算模块200可以具有TransFlash、miniSD、microSD、存储棒、压缩闪存、多媒体卡(MMC)、微型MMC、宏MMC、智能媒体、智能卡、微型智能卡、xD存储卡的物理特征(例如尺寸)，或兼容蜂窝通信设备10的其它适当外形因素。

[0037] 作为另一非限制性的例子，主机接口202可以是串行总线，例如通用串行总线(USB)接口或适合于与蜂窝通信设备110的兼容连接的“火线”接口。支持安全计算模块200可操作地耦合至个人终端设备110的其它物理配置和主机接口形式也是可行的。

[0038] 尽管安全计算模块200和个人终端设备202的物理特性(例如尺寸)可能类似于上述存储卡形式之一，但是安全计算模块200可以执行由存储卡所执行功能之外的功能，如在下文中更完整地讨论的。

[0039] 图3图示自蜂窝通信设备110断开连接的安全计算模块200。换句话说，安全计算模块200的用户可以将安全计算模块200连接至蜂窝通信设备110，随后可以将该安全计算模块200与蜂窝通信设备110断开连接。通常，使用可拆除卡的形式，用户可以手动地将安全计算模块200与蜂窝通信设备110断开连接，而不需要工具，也不需要破坏安全计算模块200。

[0040] 通过将安全计算模块200插入蜂窝通信设备110的插口从而将安全计算模块200物理地和电连接至蜂窝通信设备110，用户可以将安全计算模块200连接至蜂窝通信设备110。在一些实施例中，可以将安全计算模块200插入到在蜂窝通信设备110的外壳内形成的凹槽内。

[0041] 使用可拆除卡的形式，可以在不同的时间在多个蜂窝通信设备110内使用安全计算模块200。例如，安全计算模块200的用户可以在蜂窝通信设备110内使用安全计算模块

200，随后可以在不同的蜂窝通信设备110内使用安全计算模块200。

[0042] 图3A图示物理地和电连接至蜂窝通信设备110的安全计算模块200。在一些实施例中，安全计算模块200可以通过使用由蜂窝通信设备110提供的电力进行操作，并可以通过主机接口202(图2A)接收来自蜂窝通信设备110的电力。因此，安全计算模块200可以不被配置为当与蜂窝通信设备110断开连接时进行操作，而不是将数据存储在非易失性存储器内。在其它实施例中，安全计算模块200可以包括其自身的内部电源。

[0043] 在一些实施例中，安全计算模块200可以与基站140、网络150或服务器180直接通信。在其它实施例中，安全计算模块200可以通过主机接口202和蜂窝通信设备110，与基站140、网络150和服务器180通信。因此，蜂窝通信设备110可以接收来自安全计算模块200的信息，并将信息转发给网络150。相反地，蜂窝通信设备110可以接收来自网络150的信息，并将信息转发给安全计算模块200。

[0044] 图4图示与蜂窝通信设备110通信的安全计算模块200的简化方框图。安全通信设备110可以包括用于与主机接口202通信的接口模块508、一个或多个处理器502、电源504、存储器506、蜂窝通信器510和用户接口512。

[0045] 安全计算模块200可以包括一个或多个处理器220、存储器230、近场无线通信器240和用于在主机接口202上进行通信的接口模块250。

[0046] 可以将处理器220实施为以下项中的一种或多种：通用微处理器、专用微处理器、微控制器、其它适当的硬件，例如专用集成电路(ASIC)或现场可编程门阵列(FPGA)或其组合。这些处理器220的例子仅是说明性的，其它配置也是可行的。接口模块250配置为在主机接口202上通信，如先前所述的。

[0047] 安全计算模块200配置为执行包括计算指令的软件程序。可以配置一个或多个处理器220用于执行多种操作系统和包括用于执行本发明实施例的计算指令的应用程序。

[0048] 可以使用存储器230存储计算指令、数据和用于执行包括执行本发明各实施例的多种任务的其它信息。使用电子、磁、光、电磁或用于存储信息的其它技术，可以将存储器230实施为多种不同的形式。举例来说和非限制性的，存储器230可以包括同步随机访问存储器(SRAM)、动态RAM(DRAM)、只读存储器(ROM)、闪存、等等。

[0049] 近场无线通信器240配置为在近场无线通信信道245上与另一适当装配的近场无线通信器进行无线通信。在一些实施例中，可以将所述另一适当装配的近场无线通信器配置为另一安全计算模块200、在另一蜂窝通信设备110内配置的另一安全计算模块200、或者配置用于无线通信的销售点终端的一部分。

[0050] 安全计算模块200可以使用由蜂窝通信设备110提供的功能。例如，蜂窝通信设备110可以包括用户接口512，其包括显示器114(图1)和键盘116(图1)。因为安全计算模块200可能不具有用户接口，因此安全计算模块200可以提供用户交互数据，并指示蜂窝通信设备110在显示器114上显示信息。类似地，安全计算模块200可以请求蜂窝通信设备110向安全计算模块200提供由用户在键盘116上输入的用户交互数据。

[0051] 在一些实施例中，电源504可以将电力提供给安全计算模块200。在其它实施例中，安全计算模块200可以包括其自身的电源(未图示)。

[0052] 近场无线通信信道245可以是配置用于某些局域性通信的任意无线频率和协议。适当协议和频率的一些非限制性的例子是：适当的射频、802.1a/b/g/n型无线连接、红外、

蓝牙、射频识别(RFID)、WiFi、WiMax或其它适当的通信定义。作为非限制性的例子，将用于RFID通信的低于一英寸至若干英寸的距离直到用于蓝牙通信的大约100英尺的距离视为适当的近场距离。

[0053] 图5图示用于在个人之间执行金融交易的通信系统的简化系统图。该通信系统可以包括装配有安全计算模块(例如带有买方安全计算模块200B的买方蜂窝通信设备110B和带有卖方安全计算模块200S的卖方蜂窝通信设备110S)的两个或多个蜂窝通信设备。买方安全计算模块200B和卖方安全计算模块200S可以在近场无线通信信道245上相互通信。买方蜂窝通信设备110B可以在蜂窝通信信道112B和网络150上与其它的蜂窝通信设备、互联网或其它公共和专用网络通信。类似地，卖方蜂窝通信设备110S可以在蜂窝通信信道112S和网络150上与其它的蜂窝通信设备、互联网或其它公共和专用网络通信。

[0054] 卖方金融组织300S可以在通信信道310S上可操作地耦合至网络。类似地，买方金融组织300B可以在通信信道310B上可操作地耦合至网络。作为非限制性的例子，通信信道310B和310S可以通过互联网、蜂窝通信或其它适当的连接。在一些实施例中，卖方金融组织300S和买方金融组织300B可以是同一实体。此外，在执行金融交易时，可以将卖方金融组织300S和买方金融组织300B视为基本上类似于图1的服务器180。此外，在此可以将金融组织通称为指定者300。

[0055] 此外，图5并未图示但是本领域的普通技术人员将理解的是，卖方蜂窝通信设备110B和买方蜂窝通信设备110S通常通过如图1所示的基站140与网络150通信。

[0056] 在此图示的软件处理是为了图示在执行本发明的实施例时可以由一个或多个计算系统执行的代表性处理。除了另有规定，所描述的处理顺序不被视为限制性的。此外，可以以任意适当的硬件、软件、固件或其组合执行处理。举例来说，可以将软件处理存储在存储器230内以供执行，并由一个或多个处理器220执行。

[0057] 当作为固件或软件执行时，可以在计算机可读介质上存储或传输用于执行各处理的指令。计算机可读介质包括但是并不限于磁和光存储设备，例如盘驱动器、磁带、CD(压缩盘)、DVD(数字通用盘或数字视频盘)和半导体设备，例如RAM、DRAM、ROM、EPROM和闪存。

[0058] 此外，可以通过网络传送固件或软件。作为非限制性的例子，可以通过适当的介质提供编程，包括例如内嵌在产品中，内嵌在例如通过通信接口经由诸如通信网络(例如互联网和/或专用网络)、有线电连接、光连接和/或电磁能量等适当的传输介质传送的或者使用其它适当的通信结构或介质提供的数据信号内(例如调制载波、数据分组、数字表示等)。仅作为例子，可以作为在载波内嵌入的数据信号来传送包括处理器可用软件的示例编程。

[0059] 此外，应指出的是，可以将这些例子描述为作为流程图、程序图、结构图或方框图示出的处理。尽管流程图可以将操作描述为顺序处理，但是也可以并行或同时执行许多操作。此外，可以重新安排操作顺序。当完成其操作时，处理结束。处理可以对应于方法、函数、程序、子例程、子程序等。当处理对应于函数时，其结束对应于该函数返回调用函数或主函数。

[0060] 在用于执行金融交易的操作中，并参见图4和图5，蜂窝通信设备110用于与用户交互，以根据来自安全计算模块200的指令请求输入和显示相关信息。在安全计算模块200上执行的软件管理金融交易处理。该软件的形式可以是独立应用、设备嵌入软件，或者可以在该设备本来就有的网页浏览器内操作，所有这些均可连接至安全计算模块200。此外，软件

可以包括应用程序接口(API)、软件开发工具(SDK)或者用于生成和管理安全计算模块200的软件的其它适当的软件接口和工具。

[0061] 安全计算模块200提供用于金融交易处理所需变量的安全信息存储，例如用于签名和加密的公共和私用密钥、秘密散列密钥、一个或多个计数器变量、等。安全计算模块200还提供用于诸如散列算法、加密算法、计数器递增等的存储程序和其它适当的安全处理的安全存储器230和安全处理环境。

[0062] 因而，安全计算模块200和安全存储器230提供逻辑隔离环境，用于计算来自诸如蜂窝通信设备110和其它安全计算模块200等外部来源的散列和加密信息。

[0063] 在安全计算模块200而不是在蜂窝通信设备110上隔离地执行软件可以保护软件生成的数据免于未授权访问，例如通过在蜂窝通信设备110上安装的恶意软件，通过蜂窝通信设备110的用户，或者通过通过网络150和基站140而与蜂窝通信设备110连接的设备。

[0064] 此外，可以使用安全计算模块200验证来自外部来源的全部输入。作为非限制性的例子，安全计算模块200可以使用金融交易另一方的公共签名密钥来验证已签名的交易。

[0065] 当使用加密或散列算法时，安全计算模块200可以获知特定的加密方案或加密密钥，但是不可以被蜂窝通信设备110获知。因此，安全计算模块200可以放弃未根据该特定加密方案或使用该特定加密密钥加密的自蜂窝通信设备110接收的信息。放弃未被适当加密的信息可以防止蜂窝通信设备110与安全计算模块200交互，而不是在蜂窝通信设备110的用户接口、网络150或服务器180之间中继用户接口信息。

[0066] 处理器220可以逻辑隔离一些或全部的存储器230免于被蜂窝通信设备110内的处理器502访问。换句话说，除了通过处理器220的许可和控制，否则主机接口202无法与存储器230通信，从而防止在主机接口202(或连接至主机接口202的设备，例如蜂窝通信设备110)和存储器230之间的直接通信。此外，可以物理地隔离存储器230以免于刺探访问。

[0067] 安全计算模块200可以预先安装有保护信息，例如来自销售商、制造商或其组合的金融交易软件和保护数据(例如密钥)。此外，可以在已部署的系统上更新保护信息。

[0068] 在部署保护信息时，可以使用加密信息传输处理将保护信息传送给安全计算模块200，其中该信息可以包括数据、软件或其组合。一旦正确解密和验证了真实性(即该软件和数据源自于金融组织)，则可以在安全计算模块200内更新数据和算法(即软件程序)。

[0069] 安全计算模块200可以请求蜂窝通信设备110从服务器180(例如网络服务器、监督控制和数据获取(SCADA)服务器、公司网络服务器、金融组织300B或300S或其它服务器)中提取该软件。作为买家更新的非限制性的例子，买家蜂窝通信设备110B可以通过蜂窝通信信道112B从买家金融组织310B中提取该软件，随后将该软件提供给买家安全计算模块200B。如果需要，安全计算模块200B可以解密该软件，随后安装和执行该软件。当受到加密时，蜂窝通信设备110无法解密该加密的软件。因此，一旦提取加密软件，则蜂窝通信设备110简单地将该加密软件转发给安全计算模块200，而不解密该软件。

[0070] 安全计算模块200可以附加地或可替代地请求蜂窝通信设备110将软件或其它信息发送给服务器180(图1)。例如，安全计算模块200可以加密金融信息(例如帐号、个人身份证号码等)，将加密信息提供给蜂窝通信设备110，和指示该蜂窝通信设备110将加密信息发送给服务器180。因为在该例子中该信息是加密的，所以蜂窝通信设备110无法解密该金融信息。

[0071] 可以将驱动器软件安装在蜂窝通信设备110上，以辅助蜂窝通信设备110与安全计算模块200通信以及执行部分的金融交易。作为非限制性的例子，驱动器软件可以根据已建立的智能卡交互标准(例如PC/SC)来实现在主机接口202上的通信。作为另一个非限制的例子，驱动器软件可以执行在显示器114(图1)上的信息显示以及来自键盘116(图1)的信息提取，向安全计算模块200或者自安全计算模块200传送用户交互信息。

[0072] 安全计算模块200包括用于创建和解码安全数字签名的加密算法。此外，安全计算模块200可以包括用于加密和解密信息的加密算法。因此，存储器230的安全部分可以包括诸如加密算法、加密密钥、解密密钥、签名密钥、计数器等信息和其它适当的加密信息。

[0073] 本发明的实施例包括用于建立用于金融购买封包的安全数字签名的处理。通过结合秘密密钥来建立金融交易详情的加密安全散列，可以准备安全数字签名。可以使用与秘密密钥结合的任意加密安全散列函数来实现安全签名功能。此外，可以通过与安全计算模块200的用户关联的金融组织，定期地更新散列算法和秘密密钥。

[0074] 秘密密钥仅仅对于用户的安全计算模块200和用户的金融组织300是已知的。然而，安全计算模块200可以配置为处理多个金融账户。因此，安全计算模块200可以具有用于每个账户的秘密密钥，用于每个账户的秘密密钥将对于服务于该账户的金融组织是已知的。

[0075] 金融交易详情可以包括多种信息，例如：

[0076] 所出售的一个或多个物品的描述；

[0077] 该一个或多个物品的价格(即交易金额)；

[0078] 交易时间；

[0079] 交易日期；

[0080] 交易位置(例如通过GPS坐标，如果可用的话)；

[0081] 买家的证书和金融组织线路编号；和

[0082] 卖家的证书和金融组织线路编号。

[0083] 买家或卖家的证书可以包括信息，例如诸如帐号和金融组织标识等账户信息、公用密钥和其它适当的信息。该证书用于唯一地向金融组织标识个人。通过该处理可以维持匿名，使得买家或卖家能够向另一方保密其身份。然而，对于金融组织而言，必需唯一地标识每一方以便资金转账。如果不希望匿名，则证书还可以包括用户姓名。

[0084] 本发明的实施例包括金融购买封包(FPP)，当完全时，该封包包括金融交易详情、买家的安全数字签名和卖家的安全数字签名。

[0085] 可以使用利用秘密密钥的安全散列函数建立同时用于买家和卖家的安全数字签名。安全散列函数具有多种形式，有时由诸如国家标准和技术协会(NIST)等政府组织标准化。当新的使用秘密密钥的加密安全散列函数被标准化时，可以将它们合并在安全计算模块200内。

[0086] 在在此引入作为参考的联邦信息处理标准(FIPS)出版物198中描述了使用秘密密钥的安全散列的非限制性的例子。概括地说，可以用下式表示该散列函数：

[0087] $$HMAC_k(m) = h((K \oplus opad) \| h((K \oplus ipad) \| m))$$

[0088] 在该等式中，h是加密散列函数，K是追加有额外的零以达到散列函数的块大小的秘密密钥，m是将要认证的消息，表示为围绕有圆圈的‘+’的符号表示异或(XOR)操作，而||

表示级联，外部追加opad＝0x5c5c5c…5c5c，内部追加ipad＝0x363636…3636是两个单块长的十六进制常数。

[0089] 因而，秘密密钥是仅仅对于安全计算模块200和用户的金融组织300为已知的数字签名秘密密钥。将要认证的消息是金融交易细节以及交易号码标识符(TNI)。

[0090] 作为散列函数的补充，可选的是，可以包括第二秘密加密密钥，并将其添加给上述用于金融交易细节的物品列表，因此，其被包括在散列函数的计算之内。该补充的秘密数值还将与其它密钥资料一起存储在金融组织的安全计算模块200上。虽然将键控散列视为安全的，但是密码专家和黑客依然在继续研究破解散列和其它的加密处理。为了保证本发明的实施例更安全，可以将该第二秘密密钥包括在散列函数内，以便以安全计算模块200易于处理的方式增加所计算的安全散列的熵。

[0091] TNI是与当前交易和安全计算模块200关联的唯一号码。可以通过多种方式建立该唯一号码。作为非限制性的例子，TNI可以简单地作为由安全计算模块200执行的交易的连续递增计数。作为另一非限制性的例子，可以通过复杂算法生成TNI，例如伪随机生成的号码，只要安全计算模块200和用户的金融组织300可以生成用于当前交易的相同号码。

[0092] 因此，TNI是指给定方(例如买方或卖方)对于特定交易的所计数或所计算的交易号码，并且是在对交易签名时建立的。当买方和卖方执行不同数目的交易或者使用不同的TNI生成算法时，他们可以具有不同的交易号码。在其它实施例中，TNI对于买方和卖方可以是相同的。在这种情况下，TNI将由发起交易的一方(买方或卖方)计算，并将在另一方的数字签名处理中使用。

[0093] TNI将作为金融交易详情的一部分包括在金融购买封包签名计算内。它还将与签名的FPP一起发送给金融组织，以帮助索引该购买交易。因此，当买方对FPP签名时由买方使用的TNI可能与当卖方对FPP签名时由卖方使用的TNI不同。

[0094] 应当指出，可以在近场无线通信信道245上，在买方安全计算模块200B和卖方安全计算模块200S之间传输金融交易详情以及买方的安全数字签名和卖方的安全数字签名。近场通信无线信道245可以具有缺省的频率和协议。作为非限制性的例子，近场通信信道245可以是RFID。然而，如果缺省信道不可用，或者用户选择使用不同的信道，则可以使用另一信道。作为非限制性的例子，其它可能的通信信道是短消息服务(SMS)、多媒体消息服务(MMS)、无线应用协议(WAP)、蓝牙、WiFi和其它适当的协议。

[0095] 在一些情况下，近场通信信道245对于防止别人窃听可能不是特别安全。然而，通过同时使用买方和卖方的安全数字签名，本发明的实施例确保当前交易不受到侵害。另一方面，如果未加密，金融交易详情可能会被发现，如果在金融交易细节内存在足够信息，这可能使得窃贼获得认证。因此，一些实施例可以包括金融购买封包的加密和解密。

[0096] 加密和解密可以使用任意适当的加密算法。作为非限制性的例子，加密算法可以是对称算法，例如现有技术中公知的高级加密标准(AES)。对称加密要求仅仅对于加密者和解密者已知的秘密密钥。因此，加密可以进行以便秘密密钥是用户和用户的金融组织已知的。在这种情况下，该秘密密钥可以是用于使用散列算法建立秘密安全数字签名的相同密钥，或者它可以是用于加密/解密的不同秘密密钥。可替代地，该秘密密钥可以是在发现处理过程中确定的在买方和卖方之间的秘密密钥，如下文解释的。

[0097] 作为另一个非限制性的例子，加密算法可以是诸如现有技术中公知的RSA等非对

称算法。RSA表示首次公开该加密算法的个人的姓名首字母。在非对称加密中，使用两个密钥，公用密钥和私用密钥。用户可以使他的公用密钥对于任何人都公知，而保留他的私用密钥仅自己知道。希望向该用户发送加密消息的任何人使用该用户的公用密钥加密消息。一旦加密，仅可以通过仅仅该用户已知的私用密钥来解密该消息。

[0098] 因此，可以存在由安全计算模块200存储和管理的多个密钥，例如秘密数字签名密钥、秘密加密密钥、私用密钥和公用密钥。通常，用户并不直接更新他们的加密和签名密钥。换句话说，用户能够使用他们的密钥，但是无法篡改他们的密钥。密钥更新、添加或更改可以通过对建立安全计算模块200的服务器进行控制的组织来完成。

[0099] 为了安全地管理和更新密钥，可以在安全计算模块200内包括个人标识代码(PIC)例程，以允许用户向安全计算模块200验证自身。PIC可以包括仅用户和安全计算模块200已知的字母数字值。在另一实施例中，PIC可以是诸如指纹或视网膜扫描等某种生物统计特征的数字表示。在另一种实施例中，用户可以启动PIC输入请求，其中安全计算模块200输出一系列的字母数字字符，用户必需随后重新输入或重新打字，并提交回安全计算模块200。当然，该PIC例程可以包括输入生物统计信息和字母数字值的组合。此外，该PIC例程可以包括随机的完全自动公共图灵测试，以告知供用户输入的人机识别(CAPTCHA)算法。CAPTCHA是人类可以识别但是计算机可能无法识别的显示的倾斜和扭曲的模糊字符。

[0100] 在其它实施例中，安全计算模块200可以接收直接从附装或可附装输入设备(未图示)输入的PIC输入。这样的一个例子是通过线路直接连接至安全计算模块200的外部指纹或视网膜扫描读取器设备。这种附加硬件提供更加安全的输入，其不需要这些输入通过蜂窝通信设备110的存储器506或处理器502或包括安全计算模块200的其它计算设备。

[0101] 当安全计算模块200连接至金融组织以进行交易处理时，可以由金融组织定期地刷新用于加密/解密以及用于建立数字签名的安全散列的秘密密钥。如果如此配置，则为了重新设置密钥的目的，金融组织300可以可选地初始化与包括安全计算模块200的个人终端设备110的连接。

[0102] 作为所使用密钥的非限制性的例子，可以为每个安全计算模块200建立两个公用和私用密钥对。对于第一个密钥对，将公用密钥存储在用户的安全计算模块200内，将私用密钥存储在金融组织的安全计算模块200内。该第一密钥对允许用户的安全计算模块200加密将要发送给金融组织的信息。对于第二密钥对，将私用密钥存储在用户的安全计算模块200内，将公用密钥存储在金融组织的安全计算模块200内。该第二密钥对允许金融组织的安全计算模块200加密将要发送给用户的安全计算模块200的信息。可以使用该两个密钥对系统，以便每个用户的安全计算模块200可以具有它自己的唯一的加密通信信道，通过该加密通信信道与金融组织通信。具有用于此目的的分离密钥防止出现其中如果一条加密信道被黑客破解则全部加密信道将被黑客破解的情况。此外，因为公用密钥加密远慢于对称密钥加密，这两个密钥对可用于交换临时对称密钥，而将临时对称密钥用于特定交易。

[0103] 为了在具有安全计算模块200的两个人之间执行金融交易，首先执行发现处理，以便两个安全计算模块200相互获知。为了进行发现处理，两个安全计算模块200必需在近场无线通信器240的近场范围内。

[0104] 该发现处理开始于来自带有安全计算模块200的个人终端设备110的公开用户选项发起对于另一个人终端设备110的交易和连接。该处理通常不是简单地如在大部分RFID

支付卡和设备的情况中那样“自动的”，因为RFID处理可能本来就是不安全的，易于受到窃取、窃听和滥用。然而，在一些实施例中，可以实现与常规RFID系统的反向兼容性，以授权自动响应。作为非限制性的例子，该使用可以实现物品的自动响应，例如诸如地铁费用交易等低价交易。

[0105] 发现处理可以使用本行业中公知的若干方法中的任意种，由此查询处理查找兼容设备。当发现这样一个设备时，双方可以输入或协商相同的秘密会话密钥值等。随后，会话加密可以基于该共享的秘密密钥值。该发现和密钥协商处理的非限制性的例子是蓝牙配对和增强的蓝牙配对处理，如在现有技术中公知的。

[0106] 在安全计算模块200内包含的近场无线通信器240上执行发现处理。使安全处理器控制发送和接收信息的内容、时间和方式可以增强系统的安全性。

[0107] 可选地，可以使用常规的在线客户端-服务器方法、或者诸如安全短消息服务(SMS)协议等存储和转发格式，来执行该发现处理。

[0108] 图6是图示在已经完成发现处理之后在个人之间的金融交易期间可以执行的动作的简化流程图。应当指出，如上文解释的，可以加密或者可以不加密在买方无线通信设备110B、买方安全计算模块200B、买方金融组织300B、卖方无线通信设备110S、卖方安全计算模块200S和卖方金融组织300S中任意方之间的任意通信。

[0109] 金融交易600可以开始于买方或卖方，并可以参考图6、有时可参考图4和图5继续进行。如果买方开始金融交易600，则操作块612表示买方通过根据来自买方安全计算模块200B的指令在买方蜂窝通信设备110B上输入交易详情来创建它们。随后，买方将交易详情以及来自买方安全计算模块200B的买方证书在近场无线通信信道245上发送给卖方的安全计算模块200S。在操作块614内，卖方在卖方的蜂窝通信设备110S上查阅和批准交易详情，将卖方证书添加给交易详情，并如上文解释地使用卖方的安全数字签名对该金融购买封包数字地签名。随后，卖方在近场无线通信信道245上将该金融购买封包发送回买方。在操作块616内，买方使用买方的安全数字签名将该金融购买封包数字地签名。由买方发起的该金融购买封包现在是完整的，可选的是可以将其传送回卖方，以便卖方具有该金融购买封包的完整记录。

[0110] 如果卖方发起金融交易600，则操作块602表示卖方通过根据来自卖方安全计算模块200S的指令在卖方蜂窝通信设备110S上输入交易详情来创建它们。随后，卖方将交易详情以及来自卖方安全计算模块200S的卖方证书在近场无线通信信道245上发送给买方的安全计算模块200B。在操作块604内，买方在买方的蜂窝通信设备110B上查阅和批准交易详情，将买方证书添加给交易详情，并如上文解释地使用买方的安全数字签名将该金融购买封包数字地签名。随后，买方在近场无线通信信道245上将该金融购买封包发送回卖方。在操作块606内，卖方使用卖方的安全数字签名将该金融购买封包数字地签名。由卖方发起的该金融购买封包现在是完整的，并且可选的是可以将其传送回买方，以便买方具有该金融购买封包的完整记录。

[0111] 如果卖方或买方并未批准和数字签名该FPP，则该处理停止(未图示)。如果该交易继续，则卖方或买方可以将该金融购买封包发送给金融组织。

[0112] 判决块620确定卖方是否传送FPP。如果卖方传送该金融购买封包，则操作块622表示卖方在蜂窝通信信道112S上将该FPP发送给卖方的金融组织300S。在操作块624内，卖方

的金融组织300S通过检查卖方的安全数字签名来验证卖方。

[0113] 该验证处理使用卖方的秘密密钥对卖方的数字签名执行反向散列处理，确定交易详情是准确的，交易号码标识符是正确的，卖方的证书匹配卖方在该金融组织的账户。

[0114] 卖方的金融组织300S随后可以批准或拒绝该交易。如果拒绝，则卖方的金融组织300S将一条消息发送回卖方的蜂窝通信设备110S，该交易结束(未图示)。如果批准，则卖方的金融组织300S通过网络150将FPP和批准发送给买方的金融组织300B。在一些情况下，买方的金融组织300B和卖方的金融组织300S可以是同一实体，可能不需要通过网络150“发送”FPP。

[0115] 在操作块626内，以类似于上述用于卖方验证处理的方式，买方的金融组织300B通过使用买方的秘密密钥检查买方的安全数字签名来验证买方。随后，买方的金融组织300B可以批准或拒绝该交易。如果拒绝，则买方的金融组织300B将一条消息发送给买方的蜂窝通信设备110B，该交易结束(未图示)。如果批准，则买方的金融组织300B将资金转账给卖方的金融组织300S。

[0116] 返回判决块620，如果买方传送金融购买封包，则操作块632表示买方在蜂窝通信信道112B上将FPP发送给买方的金融组织300B。在操作块634中，如上文解释的，买方的金融组织300B通过使用买方的秘密密钥检查买方的安全数字签名来验证买家。

[0117] 随后，买方的金融组织300B可以批准或拒绝该交易。如果拒绝，则买方的金融组织300B将一条消息发送回买方的蜂窝通信设备110B，该交易结束(未图示)。如果批准，则买方的金融组织300B通过网络150将FPP和批准发送给卖方的金融组织300S。在一些情况下，买方的金融组织300B和卖方的金融组织300S可以是同一实体，可能不需要通过网络150“发送”FPP。

[0118] 在操作块636内，如上文解释的，卖方的金融组织300S通过使用卖方的秘密密钥检查卖方的安全数字签名来验证卖方。随后，卖方的金融组织300S可以批准或拒绝该交易。如果拒绝，则卖方的金融组织300S将一条消息发送给卖方的蜂窝通信设备110S，该交易结束(未图示)。如果批准，则卖方的金融组织300S将批准发送回买方的金融组织300B。在操作块638，买方的金融组织300B将资金转账给卖方的金融组织300S。在该处理的这一时刻，金融交易600已经完成。

[0119] 判决块640确定是否应当向卖方通知交易结果。如果是，则在操作块642内，卖方的金融组织300S将交易结果发送给卖方的蜂窝通信设备110S。

[0120] 如果不通知卖方，则判决块644确定是否应当向买房通知交易结果。如果是，则在操作块646，买方的金融组织300B将交易结果发送给买方的蜂窝通信设备110B，该处理完成。如果不通知买方，则该处理完成。

[0121] 在一些实施例中，买方和卖方可以通过诸如因特网等中间通信网络而不是蜂窝通信信道和近场无线通信信道来执行金融交易。在这些情况下，包含安全计算模块200的个人终端设备110可以更直接地连接至网络150。作为非限制性的例子，使用带有安全计算模块200的蜂窝通信设备110的买家可以连接至具有安全计算模块200的网站。从买家的角度来看，该交易以类似于常规互联网购买的方式进行。然而，对于通过安全计算模块200的购买，当与用户简单地输入信用卡号码相比时，包括安全数字签名的安全支付处理明显地更加安全。具有安全计算模块200的远程网站可以使用安全计算模块200软件、硬件或其组合的企

业版本。该企业版本建立了对于大量连续和同时的交易而言更加健壮的安全机制。为了确保交易之间的附加安全性，用于安全计算模块200的企业软件可以清空个人交易之间的动态交易存储器。

[0122] 在另一相关实施例中，使用带有安全计算模块200的蜂窝通信设备110的买家可以使用有线或无线连接来连接至互联网连接的计算机。该无线连接可以通过安全计算模块200的近场无线通信器240。使用该配置，买家将使用互联网连接计算机的网页浏览器选择购买一个或多个物品。在购买过程中，买家向带有安全计算模块200的网站通知该买家将使用买家本地附装的安全计算模块200执行金融交易。随后，网站将使用网站的安全计算模块200和用于安全计算模块200的企业软件执行如上文描述的交易。

[0123] 在其它相关的实施例中，可以将卖家的安全计算模块200配置为无人监管设备，可以在没有金融组织验证的情况下接受金融交易。作为非限制性的例子，可以建议允许紧急情况下的交易(例如在断电或计算机故障时销售食品)。作为另一非限制性的例子，卖家可以执行存储和转发型交易，例如由地铁终端执行的那些交易。在这些情况下，可以将交易存储在销售点的队列内，并在随后的时间内由金融组织验证。

[0124] 尽管已经参考具体实施例描述了本发明，但是本发明并不限制于这些所描述的实施例。本发明仅由权利要求书来限制，在权利要求的保护范围内包括根据所描述的本发明的原理操作的全部等同设备或方法。

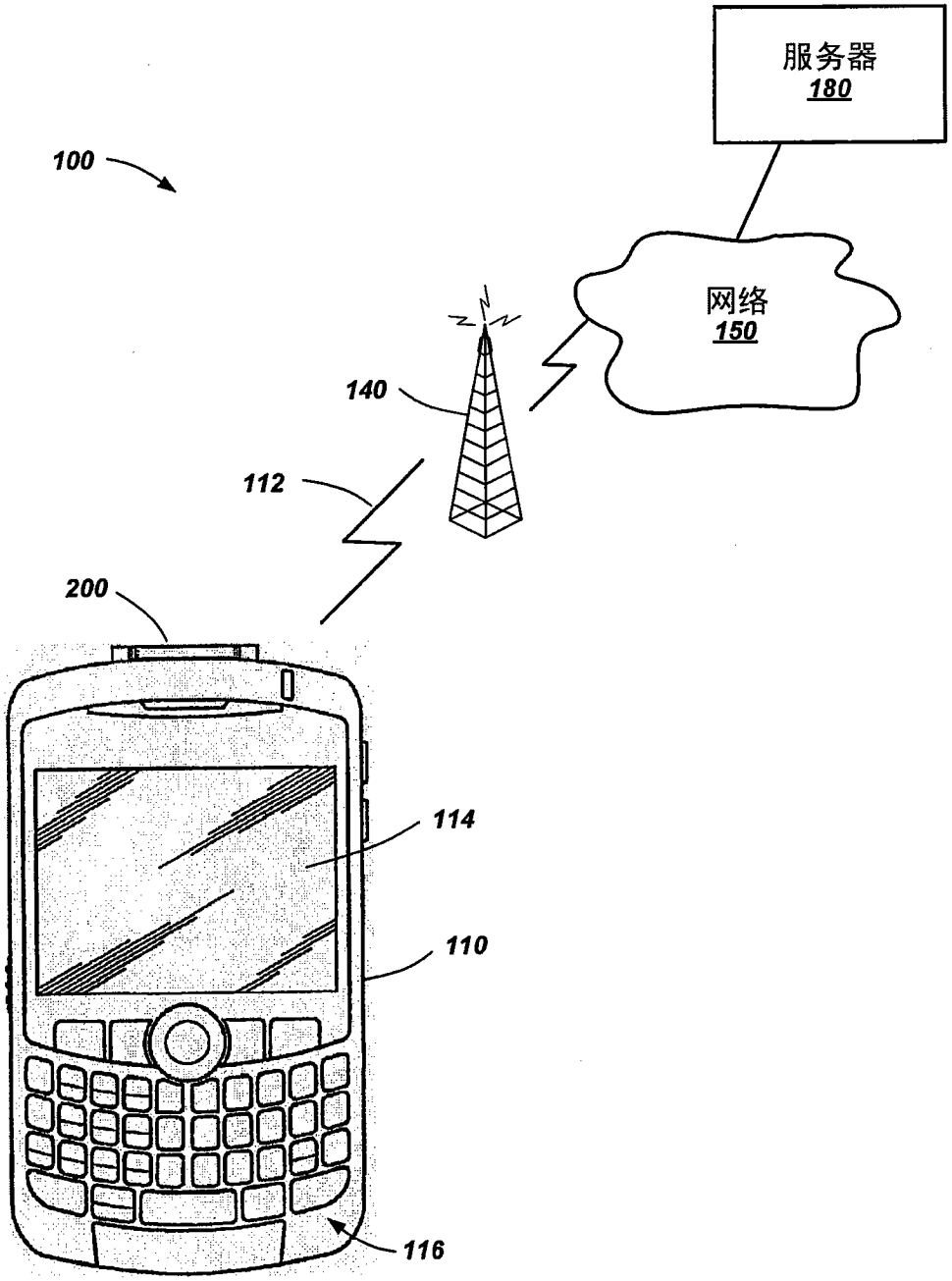


图1

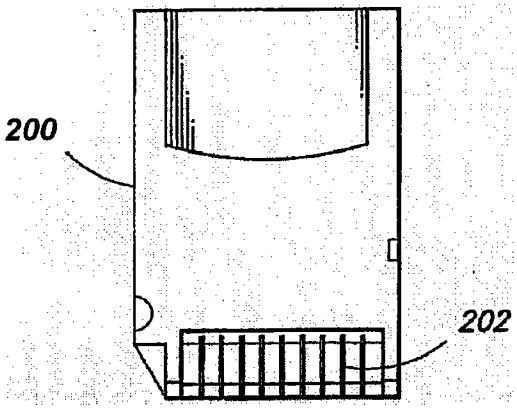


图2

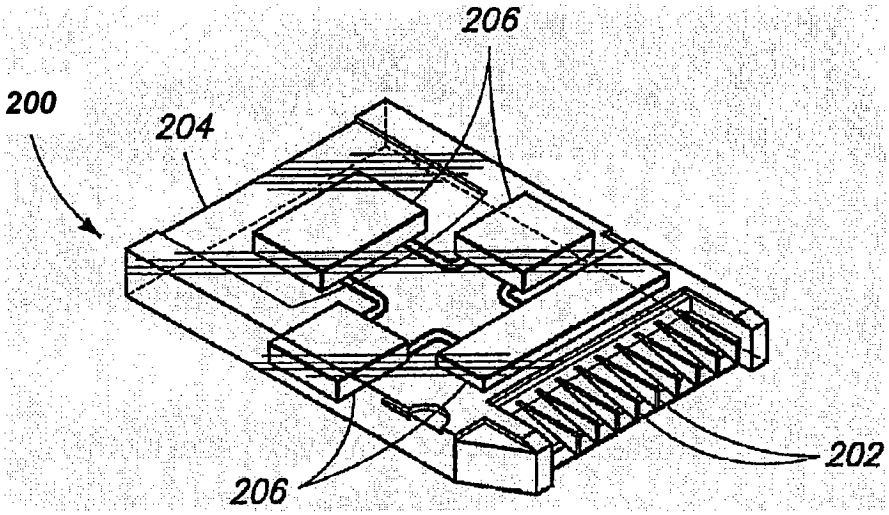


图2A

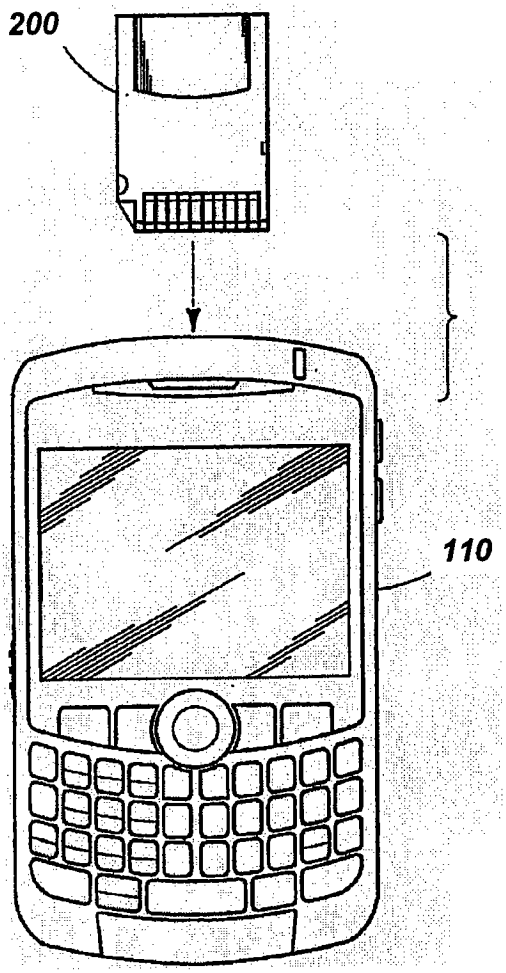


图3

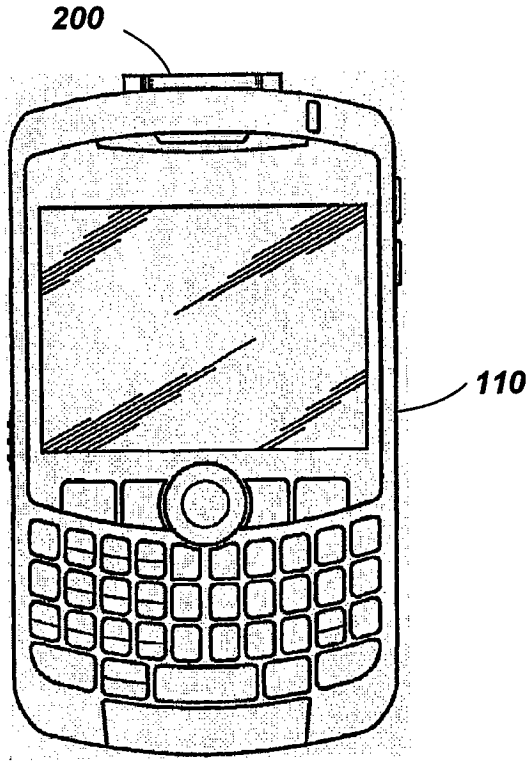


图3A

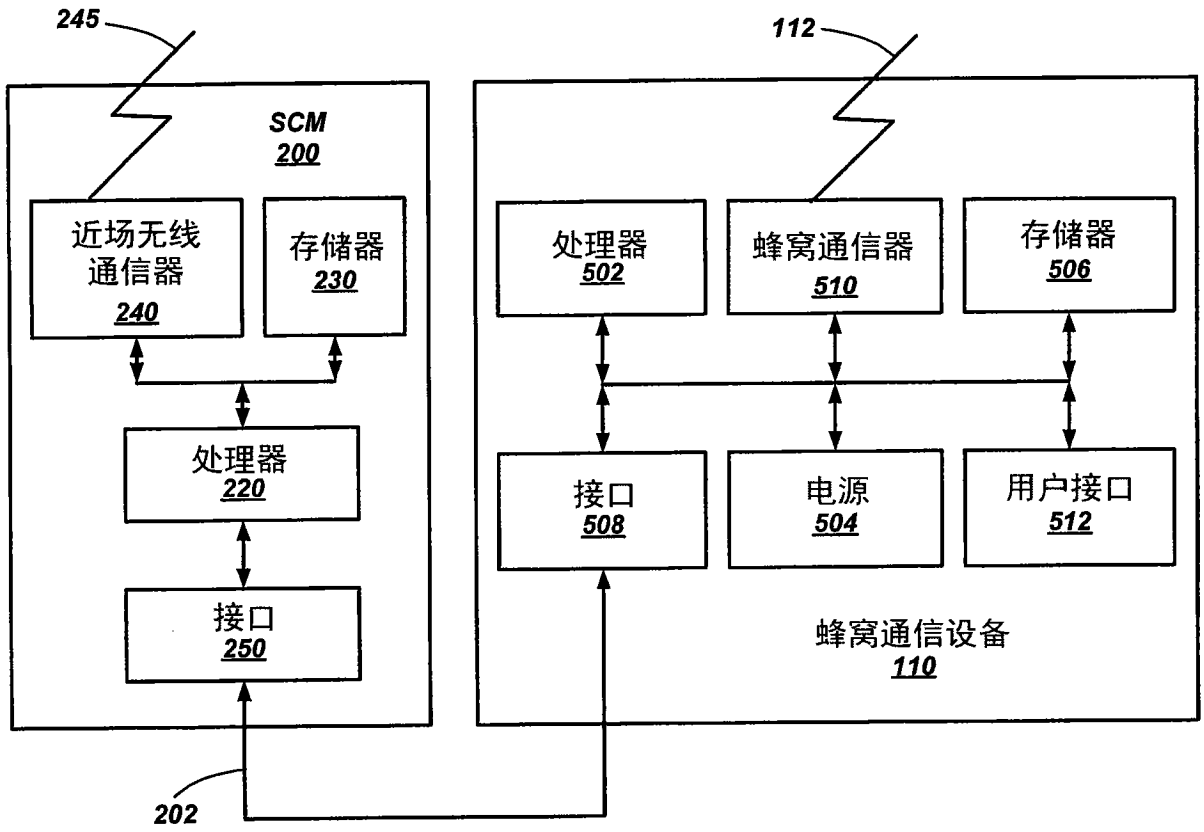

245
SCM
200
近场无线
通信器
240
存储器
230
处理器
220
接口
250
202
112
处理器
502
蜂窝通信器
510
存储器
506
接口
508
电源
504
用户接口
512
蜂窝通信设备
110

图4

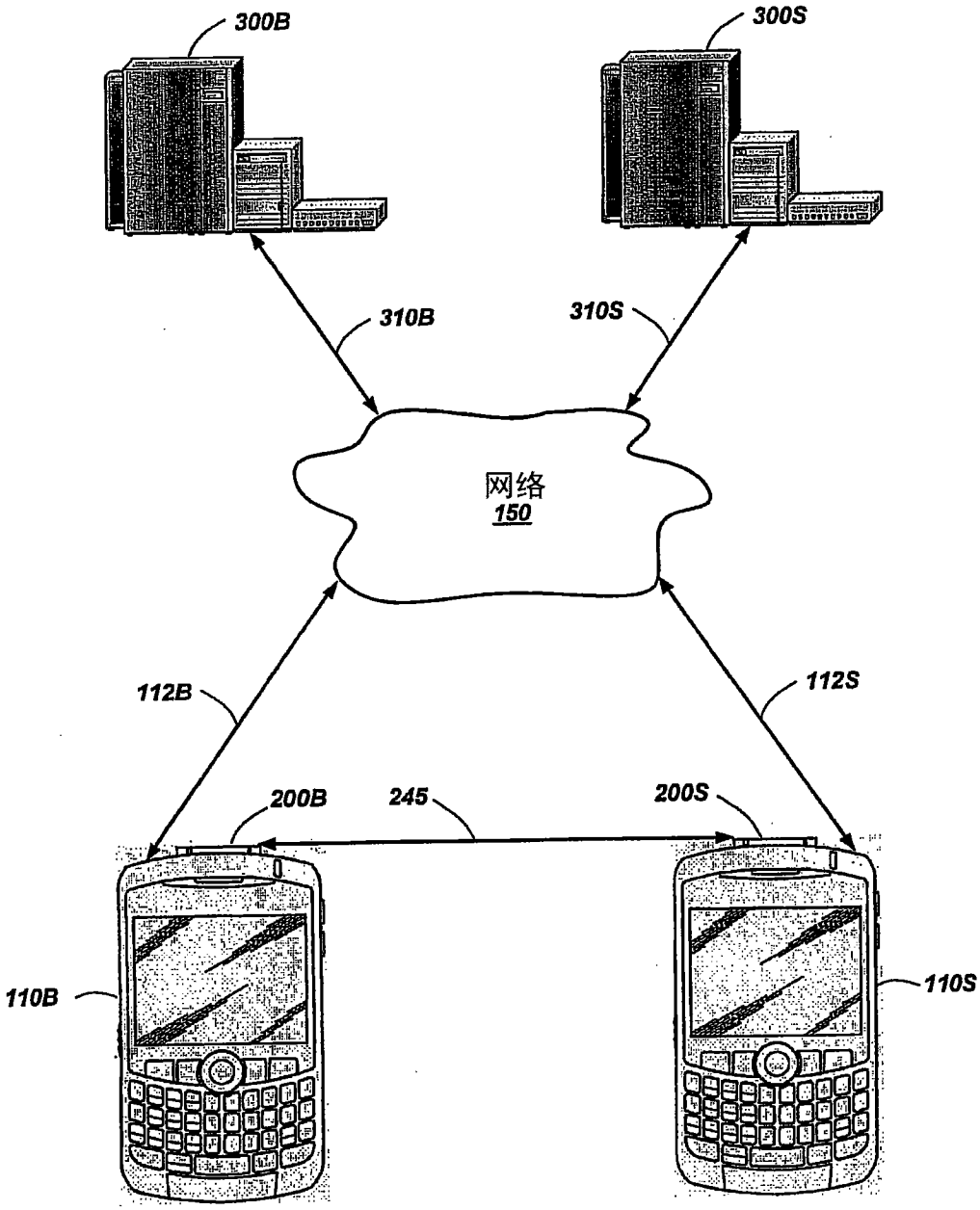


图5

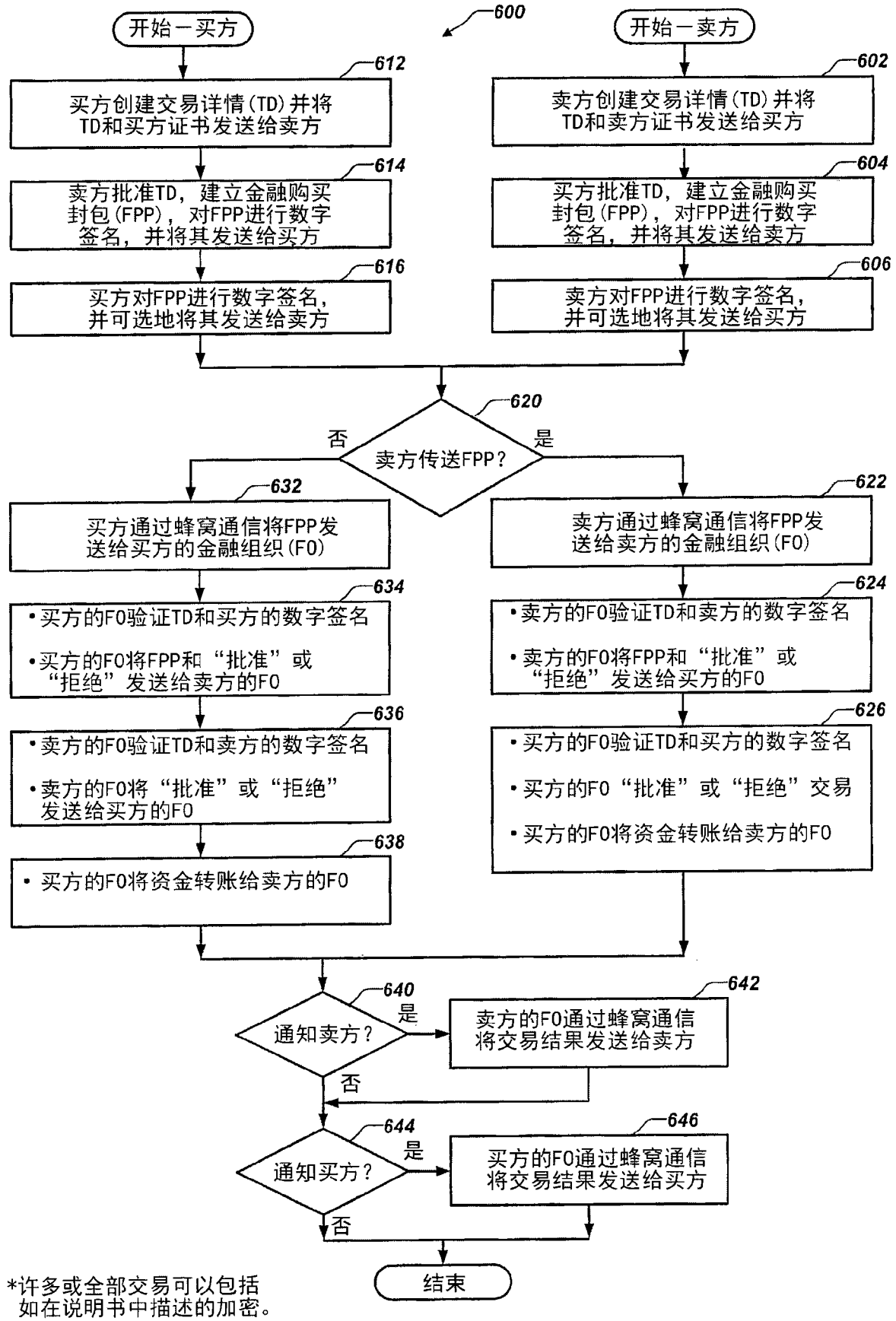

600
开始－买方
612
买方创建交易详情(TD)并将TD和买方证书发送给卖方
614
卖方批准TD，建立金融购买封包(FPP)，对FPP进行数字签名，并将其发送给买方
616
买方对FPP进行数字签名，并可选地将其发送给卖方
开始－卖方
602
卖方创建交易详情(TD)并将TD和卖方证书发送给买方
604
买方批准TD，建立金融购买封包(FPP)，对FPP进行数字签名，并将其发送给卖方
606
卖方对FPP进行数字签名，并可选地将其发送给买方
620
卖方传送FPP？
否
是
632
买方通过蜂窝通信将FPP发送给买方的金融组织(FO)
634
• 买方的FO验证TD和买方的数字签名
• 买方的FO将FPP和“批准”或“拒绝”发送给卖方的FO
636
• 卖方的FO验证TD和卖方的数字签名
• 卖方的FO将“批准”或“拒绝”发送给买方的FO
638
• 买方的FO将资金转账给卖方的FO
622
卖方通过蜂窝通信将FPP发送给卖方的金融组织(FO)
624
• 卖方的FO验证TD和卖方的数字签名
• 卖方的FO将FPP和“批准”或“拒绝”发送给买方的FO
626
• 买方的FO验证TD和买方的数字签名
• 买方的FO“批准”或“拒绝”交易
• 买方的FO将资金转账给卖方的FO
640
通知卖方？
是
否
642
卖方的FO通过蜂窝通信将交易结果发送给卖方
644
通知买方？
是
否
646
买方的FO通过蜂窝通信将交易结果发送给买方
结束
*许多或全部交易可以包括如在说明书中描述的加密。

图6