(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 101978646 B
(45)授权公告日 2016.08.03

(21)申请号 200980110155.8
(22)申请日 2009.01.28
(30)优先权数据
61/031,605 2008.02.26 US
61/031,885 2008.02.27 US
12/196,669 2008.08.22 US
(85)PCT国际申请进入国家阶段日
2010.09.20
(86)PCT国际申请的申请数据
PCT/US2009/032279 2009.01.28
(87)PCT国际申请的公布数据
WO2009/108445 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
亚伦·R·特纳
(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 王金宝
(51)Int.Cl.
H04L 9/00(2006.01)
(56)对比文件
CN 1329313 A,2002.01.02,
审查员 林姓

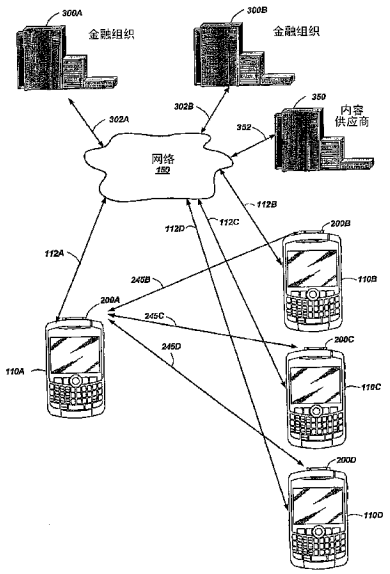
权利要求书1页 说明书16页 附图8页

(54)发明名称

用于执行文件分发和购买的系统和方法

(57)摘要

一种安全计算模块(SCM),其经配置用于与主机装置连接。所述SCM包括用于执行安全处理操作的处理器、用于将所述处理器连接至所述主机装置的主机接口以及连接至所述处理器的存储器,其中所述处理器逻辑上隔离所述主机装置对所述存储器中至少一些的访问。所述SCM产生用于金融交易的安全数字签名,并且启用通过所述主机装置接收的受控内容。从内容供应商向买方或从转售方向买方执行文件分发。所述文件分发包括使用安全数字签名和可能的消息加密的金融交易。所述数字签名和交易详情被传达至适当的金融组织以认证所述交易方并且完成所述交易。所述受控内容从所述内容供应商或所述转售方转移至所述买方。



CN 101978646 B

1.一种用于可操作连接至主机装置的安全计算模块，包含：

处理器，其用于执行安全处理操作；

主机接口，其用于将所述处理器可操作地连接至所述主机装置；以及

存储器，其可操作地连接至所述处理器，其中所述处理器逻辑上隔离所述主机装置对所述存储器中至少一些的访问；

其中所述安全计算模块经配置以：

产生用于包括金融交易详情的消息的安全数字签名；

指导所述主机装置向与所述安全计算模块用户相关的金融组织传达所述金融交易详情和所述安全数字签名；和

启用通过所述主机装置在所述安全计算模块处接收的受控内容。

2.根据权利要求1所述的安全计算模块，其中所述安全数字签名包含使用在包含所述金融交易详情和交易号码标识符的消息上的秘密密钥来产生的安全散列函数。

3.根据权利要求1所述的安全计算模块，其中所述安全计算模块进一步经配置以在与所述主机装置隔离的情况下并且在指导所述主机装置传达所述金融交易详情和所述安全数字签名之前，加密所述金融交易详情、所述安全数字签名、或其组合。

4.根据权利要求3所述的安全计算模块，其中使用所述安全计算模块和与所述用户相关的所述金融组织所知的秘密密钥以对称加密过程来执行所述加密。

5.根据权利要求3所述的安全计算模块，其中使用与所述金融组织相关的公共密钥以不对称加密过程来执行所述加密。

6.根据权利要求1所述的安全计算模块，其中所述主机装置是选自由下列各物组成的群组：蜂窝电话、智能电话、寻呼机、个人数字助理、手持计算平台、腕戴式计算系统、移动计算系统以及台式计算系统。

7.根据权利要求1所述的安全计算模块，其中所述安全计算模块进一步经配置以解密所述受控内容以供所述主机装置使用。

8.根据权利要求1所述的安全计算模块，其进一步包含近场(proximate-field)无线通信机，所述近场无线通信机可操作地连接至所述处理器并且经配置用于当处于与另一主机装置相关的另一安全计算模块的近场范围之内时与所述另一安全计算模块通信。

9.根据权利要求8所述的安全计算模块，其中所述近场无线通信机经配置以使用可用的无线电频率、红外线频率、802.1a/b/g/n型无线连接、蓝牙、RFID、WiFi、WiMax或其组合来进行通信。

10.根据权利要求8所述的安全计算模块，其中所述安全计算模块使用所述近场无线通信机来向所述另一安全计算模块传达所述金融交易详情和所述安全数字签名。

用于执行文件分发和购买的系统和方法

[0001] 相关申请

[0002] 本专利申请要求2008年8月22日提交的标题为“SYSTEMS AND METHODS FOR PERFORMING FILE DISTRIBUTION AND PURCHASE”的美国非临时专利申请第12/196,669号的权益和优先权，要求2008年2月27日提交的标题为“PHONE-TO-PHONE FILE DISTRIBUTION SYSTEM WITH PAYMENT”的美国临时专利申请第61/031,885号的权益和优先权，并且要求2008年2月26日提交的标题为“PHONE-TO-PHONE FINANCIAL TRANSACTION SYSTEM”的美国临时专利申请第61/031,605号的权益和优先权，上述申请中的每一个申请都以引用方式全文并入本文中。

[0003] 本申请还涉及2008年8月22日提交的标题为“SYSTEMS AND METHODS FOR PERFORMING WIRELESS FINANCIAL TRANSACTIONS”的美国非临时专利申请第12/196,806号(代理人案号BA-306)和同一日期提交的标题为“SYSTEMS AND METHODS FOR PERFORMING WIRELESS FINANCIAL TRANSACTIONS”的相应PCT申请(代理人案号BA-306PCT)。

[0004] 政府权力

[0005] 依据美国能源部与巴特尔能源联盟股份有限公司(Battelle Energy Alliance, LLC)之间的合约第DE-AC07-05-ID14517号，美国政府对本发明具有某些权利。

技术领域

[0006] 本发明的实施例一般涉及无线通信系统，并且更具体地说，涉及使用通信系统执行金融交易和文件分发的系统和方法。

背景技术

[0007] 多年以来，蜂窝电话是设计来主要用于提供无线语音通信。然而，随着技术上新的进展，蜂窝电话(有时称为个人无线装置)已增加了额外功能。举例而言，包括蜂窝电话、个人数字助理、电子邮件客户端、媒体播放器以及数字照相机的功能的个人无线装置现在十分普遍。由于增加了这些装置的能力，所以许多用户使用这些装置来存储或访问敏感信息(例如，金融账户信息)或用来访问专用网(例如，企业通信网)。

[0008] 就金融交易而言，对市场扩展和用户接受新颖形式的无线交易来说，极为重要的是安全性和防欺诈创新。举例而言，信用卡交易，无论亲自进行或经由互联网进行，都容易受到日益老练的窃贼欺诈和盗窃。此类攻击范围从偷取信用卡收据或复制卡号到为获取大量信用卡账号而攻击网页可访问数据库。源于这些类型攻击的欺诈每年导致数十亿美元的损失，其中既有这些最初的资金盗窃所致，也有所引起的身份盗窃所致。

[0009] 除了进行防止欺诈的工作之外，信用卡公司还不断在寻求扩展其消费者群体的新颖方法。许多的增长活动集中于吸收那些感觉需要建立信用的年轻人，诸如，那些第一次进入商场的人、有助学金来花费的大学生以及企图补救不良信用的人。

[0010] 就媒体而言，对等文件共享系统已变成寻求收益的版权持有者的祸根，因为传统的文件共享系统向消费者提供受版权保护的内容，而无需为这些作品向合法的版权持有者

进行补偿。

[0011] 需要用以支持分发受控内容(诸如,受版权保护的作品)的系统和方法,其中安全金融交易可作为分发的一部分来执行。还需要支持受控内容的个人对个人的文件共享或分发,其中安全金融交易可作为该共享或分发的一部分来执行。

发明内容

[0012] 本发明的实施例包括用于支持分发受控内容的系统和方法,其中安全金融交易可作为该分发的一部分来执行。本发明的实施例还支持受控内容的个人对个人的文件共享或分发,其中安全金融交易可作为共享或分发的一部分来执行。

[0013] 在本发明的一个实施例中,安全计算模块经配置用于可操作连接至主机装置。该安全计算模块包括用于执行安全处理操作的处理器、用于可操作地将处理器连接至主机装置的主机接口以及可操作地连接至处理器的存储器,其中该处理器逻辑上隔离主机装置对存储器中的至少一些的访问。该安全计算模块经配置以产生用于包括金融交易详情的消息的安全数字签名。该安全计算模块还经配置以指导该主机装置向与安全计算模块用户相关的金融组织传达金融交易详情和该安全数字签名并且启用通过该主机装置接收的受控内容。

[0014] 根据本发明的另一个实施例,执行文件分发的方法包括选择将从作为卖方的内容供应商处接收的受控内容。向买方发送关于该受控内容的金融交易详情。该方法还包括通过使用买方的安全计算模块用买方的安全数字签名来签署所述金融交易详情和通过使用卖方的安全计算模块用卖方的安全数字签名来签署所述金融交易详情。金融交易详情、买方的安全数字签名以及卖方的安全数字签名构成金融交易包。该方法还包括在买方与卖方之间传达该金融交易包、向卖方的金融组织传达该金融交易包以及向买方的金融组织传达该金融交易包。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,并且向买方的金融组织发送卖方许可。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、向卖方的金融组织发送买方许可以及执行从买方的金融组织向卖方的金融组织的资金转移。该方法还包括将受控内容从内容供应商传达至买方的安全计算模块。

[0015] 根据本发明的另一个实施例,执行文件分发的方法包括选择将从转售方接收的受控内容、确定包括交易量和该受控内容的内容所有者的金融交易详情以及向买方发送关于该受控内容的金融交易详情。该方法还包括通过使用买方的安全计算模块用买方的安全数字签名来签署所述金融交易详情和通过使用转售方的安全计算模块用转售方的安全数字签名来签署所述金融交易详情。金融交易详情、买方的安全数字签名以及转售方的安全数字签名构成金融交易包。该方法还包括在买方与转售方之间传达该金融交易包、向买方的金融组织传达该金融交易包以及向内容所有者的金融组织传达该金融交易包。该内容所有者的金融组织验证金融交易详情并且向买方的金融组织发送卖方许可。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、向内容所有者的金融组织发送买方许可以及执行从买方的金融组织向内容所有者的金融组织的资金转移。该方法还包括将受控内容从转售方的安全计算模块传达至买方的安全计算模块。

附图说明

[0016] 图1表示包括主机装置和安全计算模块的通信系统；

[0017] 图2表示体现为适于插入蜂窝通信装置的卡片的安全计算模块的前视图；

[0018] 图2A用半透视图表示图2的安全计算模块的等距视图，以表示根据本发明实施例的内部元件；

[0019] 图3表示从蜂窝通信装置上分离的安全计算模块；

[0020] 图3A表示实体上和电气上连接至蜂窝通信装置的安全计算模块；

[0021] 图4表示与蜂窝通信装置通信的安全计算模块的简化框图；

[0022] 图5表示用于在个体之间执行金融交易和受控内容分发的通信系统的简化系统图；

[0023] 图6是表示在从内容供应商分发和购买受控内容期间可执行的动作的简化程序框图；以及

[0024] 图7A和图7B是表示在个体之间分发和购买受控内容期间可执行的动作的简化程序框图。

具体实施方式

[0025] 在以下详细说明中，结合形成本文一部分的附图进行描述，并且其中通过举例说明示出了可以实施本发明的多个具体实施例。足够详细地描述了这些实施例，以使得所属领域的技术人员能够实施本发明。然而，应当理解的是，当指示本发明实施例的实例时，该详细说明和所述具体实例是仅以举例说明方式而非限制性方式来给出。根据本发明，可以在本发明范围之内进行各种代替、修改、添加、重新布置、或对其进行组合，并且对所属领域的技术人员将为显而易见。

[0026] 本发明的实施例包括用于支持分发受控内容的系统和方法，其中安全金融交易可作为该分发的一部分来执行。本发明的实施例还支持受控内容的个人对个人的文件共享或分发，其中安全金融交易可作为该共享或分发的一部分来执行。另外，本发明的实施例提供为受控内容的法定持有者收集并保存市场接受的财务收入(例如，版税、报酬等)的系统和方法。此外，本发明的实施例提供用于完善和批准个人对个人的营销、销售以及分发机制的系统和方法，以便鼓励用户使用个人对个人的发现和分发方法来合法地共享和传播受控内容。

[0027] 通过增加具有软件和用于执行该软件的安全计算模块(SCM)的个人电子装置(PEDs)，所述系统和方法包括受控内容分发和安全金融交易。该SCM可以是可嵌入或已嵌入该PED的处理硬件。

[0028] 如本文所用，PED可以是用户使用的任何移动计算装置，并且能够使用蜂窝无线通信通道进行通信。PED在本文中也可以称为主机装置、蜂窝通信装置、或无线通信装置。PED的实例包括蜂窝电话、智能电话、Blackberry ®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)、手持计算平台、腕戴式计算系统、或其他的移动计算系统(例如，膝上计算机)。另外，主机装置可以是配备有安全计算模块的台式计算机、服务器、或其他的装置，诸如卫星电视接收器、数字多功能光盘(DVD)播放器以及盒式录像机(VCRs)。虽然本文大部分描述集中于将PED作为无线通信装置，但所属领域的技术人员将认识到，任何适当的主机装置都可经配置来与安全计算模块一起操作以实施本发明的实施例。

[0029] 如本文所用，“受控内容”涉及任何受版权保护的材料或可认为具有版权的任何材料。此类实例包括(但不限于)以下这些：音乐、视频、电子书、软件、文档、地图、数据库、商店折扣券、商人忠诚度材料、照片、或其他数字内容。此外，受控内容包括访问授权令牌。作为非限制性实例，访问授权令牌可以包括用于准许进入电影、音乐会、体育赛事等场所的电子票(即，e-票)。

[0030] 如本文所用，“内容所有者”是根据本国法、国际法或其组合对受控内容可拥有至少一些权利的实体或个体，内容所有者可控制对受控内容的访问、自己创造受控内容，或合法购买受控内容。

[0031] 如本文所用，“内容供应商”是内容所有者或该内容所有者的代理人，其经授权以提供该内容所有者拥有的受控内容。

[0032] 如本文所用，“分发规则”是定义分发权利和方法的规则。此类规则可以限制对特定群体的分发、时间周期、数量等。

[0033] 如本文所用，“原始买方”是直接从内容所有者或该内容所有者的代理人处购买受控内容的买方。

[0034] 如本文所用，“转售方”是经授权以根据该内容所有者规定的分发规则来转售受控内容的买方。

[0035] 图1表示包括主机装置110、服务器180、网络150、无线通信基站140以及安全计算模块200的通信系统100。

[0036] 在一些实施例中，主机装置110可以是蜂窝通信装置110。蜂窝通信装置110可以使用可为蜂窝无线通道的无线通道112来与基站140通信。蜂窝通信装置110可以是无线通信装置，诸如经配置以与陆地蜂窝基站140通信的智能手机、Blackberry ®智能手机、膝上计算机、或其他适当装置。基站140可以与网络150通信。网络150可以是通信网络，诸如互联网、公用交换电话网、或用于实施通信的任何其他适当布置。

[0037] 蜂窝通信装置110可以包括用于向用户传达信息的显示器和用于用户向蜂窝通信装置110传达信息的键盘。

[0038] 安全计算模块200可以实体上连接至蜂窝通信装置110。作为非限制性实例，安全计算模块200可以经配置为适于插入主机装置110中的卡片。虽然实体上连接至主机装置110，但安全计算模块200可以独立地执行软件和/或与主机装置110隔离。

[0039] 图2表示体现为适于插入蜂窝通信装置100的卡片的安全计算模块200的前视图。图2A用半透视图表示图2的安全计算模块200的等距视图，以表示根据本发明实施例的内部元件。安全计算模块200可以具有类似于安全数字(SD)存储卡的物理特征。举例而言，安全计算模块200可以包括尺寸大体上类似于SD存储卡的外壳204。此外，安全计算模块200可以包括经配置以实体上和电气上连接至蜂窝通信装置110的主机接口202。作为非限制性实例，主机接口202可以经配置为SD输入/输出(SDIO)接口、安全数字高容量(SDHC)接口、或适于插入扩展物(其适于插入蜂窝通信装置110的SD槽)的其他接口。如图2A所示，安全计算模块200可以包括外壳204、电路206以及主机接口202。

[0040] 外壳204围绕电路206，并且可通过将电路206包围在其中以使得电路206实体上并未暴露于用户，从而允许用户处理安全计算模块200而不会损坏电路206。

[0041] 如图2和图2A所示，可以将一些实施例配置来使得包括安全计算模块200的外壳

204不同于主机装置110并且可从主机装置110上拆卸。在其他实施例中，安全计算模块200可以不包括外壳，并且可以嵌入蜂窝通信装置110中。在任何实施例中，安全计算模块200经配置以维持与蜂窝通信装置110至少逻辑上的隔离，如下文更全面阐述那样。

[0042] 电路206可以包含一或多个集成电路，并且可以包含一或多个电路板。电路206可以经配置以执行安全计算模块200的功能。

[0043] 当然，可以用不同于SD形状因数的形状因数来配置安全计算模块200。举例而言，安全计算模块200可以具有TransFlash、miniSD、microSD、存储棒、紧凑式闪存、多媒体卡(MMC)、缩小尺寸MMC、微MMC、智能媒体、智能卡、迷你智能卡、xD存储卡的物理特征(例如，尺寸)、或与蜂窝通信装置110兼容的其他适当形状因数。

[0044] 作为另一个非限制性实例，主机接口202可以是串行总线，诸如适于兼容连接至蜂窝通信装置110的通用串行总线(USB)接口或“火线”接口。还可能存在允许安全计算模块200可操作地连接至主机装置110的其他实体配置和主机接口格式。

[0045] 虽然安全计算模块200和主机接口202的物理特征(例如，尺寸)类似于上述存储卡格式中的一种格式，但安全计算模块200可以执行比存储卡所执行的功能更多的功能，如下文更全面论述那样。

[0046] 图3图示与蜂窝通信装置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连接至蜂窝通信装置110，并且以后可将安全计算模块200与蜂窝通信装置110断开连接。通常，通过可拆卸卡格式，用户可以用手而不用工具将安全计算模块200与蜂窝通信装置110断开连接，并且不会损坏安全计算模块200。

[0047] 用户可以通过将安全计算模块200插入蜂窝通信装置110的插座中从而将安全计算模块200实体上和电气上连接至蜂窝通信装置110，来将安全计算模块200连接至蜂窝通信装置110。在一些实施例中，可以将安全计算模块200插入在蜂窝通信装置110的外壳内形成的槽中。

[0048] 通过可拆卸卡格式，可以在不同时刻将安全计算模块200用于大于一种的蜂窝通信装置110中。举例而言，安全计算模块200的用户可以在蜂窝通信装置110中使用安全计算模块200，并且之后在不同的蜂窝通信装置110中使用该安全计算模块200。

[0049] 图3A图示实体上和电气上连接至蜂窝通信装置110的安全计算模块200。在一些实施例中，安全计算模块200可以通过使用蜂窝通信装置110供给的电力来操作，并且可以经由主机接口202(图2A)从蜂窝通信装置110接收电力。因此，安全计算模块200可能不会经配置以在与蜂窝通信装置110断开连接时操作，而是将数据存储于非易失性存储器中。在其他实施例中，安全计算模块200可以包括其自身的内部电源。

[0050] 在一些实施例中，安全计算模块200可以直接与基站140、网络150、或服务器180通信。在其他实施例中，安全计算模块200可以通过主机接口202和蜂窝通信装置110来与基站140、网络150以及服务器180通信。因此，蜂窝通信装置110可以从安全计算模块200接收信息，并且将该信息转发至网络150。相反地，蜂窝通信装置110可以从网络150接收信息，并且将该信息转发至安全计算模块200上。

[0051] 图4图示与蜂窝通信装置110通信的安全计算模块200的简化框图。蜂窝通信装置110可以包括用于与主机接口202通信的接口块508、一或多个处理器502、电源504、存储器506、蜂窝通信机510以及用户接口512。

[0052] 安全计算模块200可以包括一或多个处理器220、存储器230、近场(proximate-field)无线通信机240以及用于在主机接口202上进行通信的接口块250。

[0053] 处理器220可以经实施为以下中的一或多个：通用微处理器、专用微处理器、微控制器、其他适当硬件，诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA)、或其组合。处理器220的这些实例是用于举例说明，并且可能存在其他的配置。接口块250经配置以在主机接口202上进行通信，如先前所描述那样。

[0054] 安全计算模块200经配置用于执行包含计算指令的软件程序。一或多个处理器220可以经配置用于执行包括用于实施本发明的实施例的计算指令的各种各样的操作系统和应用程序。

[0055] 存储器230可以用于保存用于执行包括执行本发明实施例在内的各种各样任务的计算指令、数据以及其他信息。可以通过使用用于存储信息的电子技术、磁性技术、光学技术、电磁技术、或其他技术来将存储器230体现为若干不同形式。作为举例而非限定，存储器230可能包括同步随机存储器(SRAM)、动态RAM(DRAM)、只读存储器(ROM)、闪速存储器等。

[0056] 近场无线通信机240经配置用于经由近场无线通信通道245与另一个适当装备的近场无线通信机进行无线通信。在一些实施例中，其他适当装备的近场无线通信机可以经配置为以下各项的一部分：另一个安全计算模块200、配置在另一个蜂窝通信装置110中的另一个安全计算模块200、或配置用于无线通信的出售点终端。

[0057] 安全计算模块200可以使用蜂窝通信装置110提供的功能。举例而言，蜂窝通信装置110可以包括用户接口512，该用户接口512包含显示器114(图1)和键盘116(图1)。由于安全计算模块200可能不具有用户接口，所以安全计算模块200可以提供用户交互数据，并且指示蜂窝通信装置110在显示器114上显示信息。类似地，安全计算模块200可以请求蜂窝通信装置110向安全计算模块200提供用户通过键盘116输入的用户交互数据。

[0058] 在一些实施例中，电源504可以向安全计算模块200提供电力。在其他实施例中，安全计算模块200可以包括其自身的电源(未示出)。

[0059] 近场无线通信通道245可以是配置用于一定程度上局部的通信的任何无线频率和协议。适当的协议和频率的一些非限制性实例是：适当的无线电频率、802.1a/b/g/n型无线连接、红外线频率、蓝牙®、无线电频率识别(RFID)、WiFi、WiMax、或其他适当的通信定义。作为非限制性实例，适当的近场范围考虑为用于RFID通信的小于一英寸至几英寸的距离和用于蓝牙®通信的高达约100英尺的距离。

[0060] 图5图示用于在个体之间执行金融交易和受控内容分发的通信系统的简化系统图。通信系统可以包括配备有安全计算模块的两个或两个以上蜂窝通信装置。该通信系统可以包括有包括第一安全计算模块200A的第一主机装置110A和额外的主机装置，诸如，包括第二安全计算模块200B的第二主机装置110B、包括第三安全计算模块110C的第三主机装置110C以及包括第四安全计算模块200D的第四主机装置110D。

[0061] 为便于描述，取决于所执行的操作和操作的背景，可能以不同方式提及第一主机装置110A和第一安全计算模块200A。举例而言，在原始买方从内容供应商购买受控内容的背景下，第一主机装置110A和第一安全计算模块200A可以分别称为买方的主机装置110A和买方的安全计算模块200A。作为另一个实例，在转售方向另一个买方提供受控内容的背景下，第一主机装置110A和第一安全计算模块200A可以分别地称为转售方的主机装置110A和

转售方的安全计算模块200A。

[0062] 安全计算模块(一般指定为200)可以使用近场无线通信通道(例如245B、245C和245D)与另一个安全计算模块200通信。任何主机装置(一般指定为110)可以与网络通信,这可以经由有线或无线通信来实现。对蜂窝通信装置来说,可以经由蜂窝通信通道112A、112B、112C以及112D来进行通信。

[0063] 第一金融组织300A可以经由通信通道302A可操作地连接至网络。类似地,第二金融组织300B可以经由通信通道302B可操作地连接至网络,并且内容供应商350可以经由通信通道352可操作地连接至网络。作为非限制性实例,通信通道302A、302B和352可以通过互联网、蜂窝通信、电话网络、或其他适当的连接来实现。

[0064] 取决于背景,第一金融组织300A可以称为买方的金融组织或转售方的金融组织,如在下文描述中将显而易见那样。类似地,取决于背景,第二金融组织300B可以称为内容供应商的金融组织、卖方的金融组织、或买方的金融组织,如在下文描述中将显而易见那样。

[0065] 在一些实施例中,卖方的金融组织和买方的金融组织可以是相同的实体。此外,在金融交易的执行中,可以将卖方金融组织和买方的金融组织考虑为大体上类似于图1的服务器180。另外,本文中,金融组织一般可以用指示符300来提及。

[0066] 虽然图5未作图示,但所属领域的技术人员将理解的是,当主机装置(110A-110D)是蜂窝装置时,蜂窝通信通道(112A-112D)通常经由基站140来与网络150通信,如图1图示的那样。

[0067] 本文举例说明的软件过程旨在说明可在实施本发明的实施例中通过一或多个计算系统来执行的代表性过程。除非另外指明,否则不应将描述这些过程的顺序理解为一种限制。此外,可以采用任何适当的硬件、软件、固件、或其组合来实施这些过程。举例而言,软件过程可以存储在存储器230中以用于执行,并且可以通过一或多个处理器220来执行。

[0068] 当作为固件或软件来执行时,用于执行这些过程的指令可以存储在计算机可读媒体上或在其上转移。计算机可读媒体包括(但不限于)磁性和光学存储装置(诸如,磁盘驱动器、磁带、CD(高密度磁盘)、DVD(数字多功能光盘或数字视频光盘)和半导体装置(诸如,RAM、DRAM、ROM、EPROM以及闪速存储器)。

[0069] 另外,固件或软件可以经由网络来进行传达。作为非限制性实例,编程可以经由恰当的媒体来提供,该媒体包括(例如)体现在制品之内的媒体、体现在经由恰当的传输媒体来传达的数据信号(例如,已调制的载波、数据包、数字表示等)之内的媒体,该恰当的传输媒体为(例如)经由通信接口提供的诸如通信网络(例如,互联网和/或专用网)、有线电气连接、光学连接和/或电磁能之类,或者该编程可以通过其他恰当的通信结构或媒体来提供。在一个实例中,包括处理器可用软件的示例性编程可以作为体现为载波的数据信号来进行传达。

[0070] 另外,应注意的是,这些实例可以作为图示成流程图、程序框图、结构图、或框图的过程来描述。虽然流程图可能将操作描述为顺序过程,但许多操作可并行或同时地执行。另外,操作的顺序可以重新布置。当过程的操作完成时,该过程终止。过程可以对应于方法、功能、规程、子例程、子程序等。当过程对应于功能时,其终止对应于该功能返回至呼叫功能或主要功能。

[0071] 在用于执行受控内容分发和金融交易的操作中且参见图4和图5,主机装置110用

于与用户接口连接以请求输入并且在安全计算模块200的指导下显示相关信息。在安全计算模块200上执行的软件管理金融交易过程和受控内容转移。该软件可以为独立应用程序、装置嵌入软件的形式，或可以在装置本身的网页浏览器之内操作，所述程序、软件和浏览器都可连接至安全计算模块200。另外，软件可以包括用于产生和管理安全计算模块200的软件的应用程序接口(API)、软件开发工具包(SDK)或其他适当的软件接口以及工具。

[0072] 安全计算模块200为金融交易过程所需的变量(诸如，用于签署和加密的公共和私人密钥、秘密散列密钥、计数器变量等)提供安全信息存储。安全计算模块200还为存储的程序(诸如，散列算法、加密算法、计数器递增以及其他适当的安全过程)提供安全存储器230和安全处理环境。

[0073] 因此，安全计算模块200和安全存储器230提供逻辑上隔离的环境，以计算散列并且加密来自诸如主机装置110和其他安全计算模块200的外部源的信息。

[0074] 在隔离中在安全计算模块200上执行该软件而不是在主机装置110上执行该软件可以保护该软件产生的数据免受下列这些进行未授权访问：例如，主机装置110上安装的恶意软件、主机装置110的用户，或可通过网络150和基站140连接至主机装置110的装置。

[0075] 另外，安全计算模块200可以用于批准所有来自外部源的输入。作为非限制性实例，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签署的交易。

[0076] 当使用加密或散列算法时，可以通过安全计算模块200而不是通过主机装置110来获知具体的加密方案或加密密钥。因此，安全计算模块200可以忽略从主机装置110接收到的未根据具体加密方案或未用具体的加密密钥来加密的信息。忽略未恰当加密的信息可以阻止主机装置110与安全计算模块200互动，而不阻止在主机装置110的用户接口、网络150、或服务器180之间中继用户接口信息。

[0077] 处理器220可以逻辑上隔离主机装置110中的处理器502对存储器230中的一些或所有的访问。换句话说，除非经由处理器220许可和控制，否则主机接口202可能不能与存储器230通信，从而阻止主机接口202(或连接至主机接口202的装置，诸如主机装置110)与存储器230之间的直接通信。另外，存储器230可以在实体上隔离窥探访问。

[0078] 安全计算模块200可以预安装受保护信息，诸如来自出售者、制造商、或其组合的金融交易软件和受保护数据(例如，密钥)。另外，可以在已部署的系统上更新该受保护信息。

[0079] 在部署受保护信息时，可以使用已加密信息转移过程将受保护信息传达至安全计算模块200，其中信息可以包括数据、软件、或其组合。在有效解密和真实性验证(即，金融组织处产生的软件和数据的真实性)之后，可以在安全计算模块200内更新数据和算法(即，软件规程)。

[0080] 安全计算模块200可以请求主机装置110从服务器180(例如，万维网服务器、监控和数据采集(SCADA)服务器、企业通信网服务器、金融组织300A或300B、或其他服务器)处取得该软件。作为买方更新的非限制性实例，买方的主机装置110A可以经由蜂窝通信通道112A从买方的金融组织300A处取得该软件，然后向买方的安全计算模块200A提供该软件。如有必要，安全计算模块200A可以加密该软件，然后安装并且执行该软件。如果已加密，则主机装置110不能解密该已加密软件。因此，在取得已加密软件之后，主机装置110仅向安全计算模块200转发该已加密软件，而不解密该软件。

[0081] 安全计算模块200可以另外或替代地请求主机装置110向服务器180(图1)发送软件或其他信息。举例而言,安全计算模块200可以加密金融信息(例如、账号、个人标识号等),向主机装置110提供该已加密信息,并且指示主机装置110向服务器180发送该已加密信息。在该实例中,由于该信息已加密,所以主机装置110可能不能解密该金融信息。

[0082] 可以在主机装置110上安装驱动软件以协助主机装置110与安全计算模块200通信和执行部分金融交易。作为非限制性实例,根据建立的智能卡交互标准(例如,PC/SC),驱动软件可以在主机接口202上启用通信。作为另一个非限制性实例,驱动软件可以执行显示器114(图1)上的信息呈现和从键盘116(图1)的信息获取,并且向安全计算模块200或从安全计算模块200传达该用户交互信息。

[0083] 安全计算模块200包括用于产生和解码安全数字签名的密码算法。另外,安全计算模块200可以包括用于加密和解密信息的密码算法。因此,存储器230的安全部分可以包括诸如以下这些信息:密码算法、加密密钥、解密密钥、签署密钥、计数器以及其他适当的密码信息。

[0084] 本发明的实施例包括用于产生针对金融购买包的安全数字签名的过程。安全数字签名可以通过结合秘密密钥以产生金融交易详情的密码安全散列来准备。任何结合秘密密钥的密码安全散列函数可以用于实现该安全签署功能。此外,散列算法和秘密密钥可以由与安全计算模块200的用户相关的金融组织周期性地更新。

[0085] 秘密密钥仅为用户的安全计算模块200和用户的金融组织300所知。然而,安全计算模块200可以经配置以处理多个金融账户。因此,安全计算模块200可以具有用于各账户的秘密密钥,并且该用于各账户的秘密密钥将为服务于该账户的金融组织所知。

[0086] 金融交易详情可以包括各种信息,诸如:

[0087] 对正在出售项目的描述;

[0088] 所述项目的价格(即,交易量);

[0089] 交易时间;

[0090] 交易日期;

[0091] 交易地点(例如,经由GPS坐标,如果可用的话);

[0092] 买方的凭证和金融组织路由号码;以及

[0093] 卖方的凭证和金融组织路由号码。

[0094] 买方或卖方的凭证可以包括诸如以下的信息:诸如账号和金融组织标识之类的账户信息、公共密钥以及其他适当的信息。这些凭证用于向金融组织唯一地识别个人。该过程中可以维持匿名,从而允许买方或卖方对另一方保留其身份。然而,各方必须以资金转移顺序依次向金融组织唯一地识别。如果不期望匿名,则凭证也可包括该用户的名称。

[0095] 本发明的实施例包括金融购买包(FPP),当完成时,该FPP包括金融交易详情、买方的安全数字签名以及卖方的安全数字签名。

[0096] 用于买方和卖方两者的安全数字签名可以通过使用秘密密钥用安全散列函数来产生。安全散列函数具有许多形式,并且有时通过诸如国家标准技术研究所(NIST)之类的政府单位进行标准化。当使用秘密密钥的新密码安全散列函数经过标准化时,可将其并入安全计算模块200中。

[0097] 使用秘密密钥的安全散列的非限制性实例在联邦信息处理标准(FIPS)出版物198

中有所描述，该出版物以引用方式并入本文。一般地说，该散列函数可以由以下方程式代表：

[0098] $$\mathrm{HMAC}_K(m) = h\Big((K \oplus \mathrm{opad}) \| h((K \oplus \mathrm{ipad}) \| m)\Big)$$

[0099] 在该方程式中，h是密码散列函数，K是用额外的零填充至散列函数块大小的秘密密钥，m是待认证的消息，示出的具有环绕在周围的圆圈的“+”符号表示异或(XOR)操作，同时||表示拼接，并且外部填充opad＝0x5c5c5c...5c5c，且内部填充ipad＝0x363636...3636是两个“一个块长”的十六进制常数。

[0100] 因此，该秘密密钥是仅为安全计算模块200和用户的金融组织300所知的数字签名秘密密钥。待认证消息是连同交易号码标识符(TNI)一起的金融交易详情。

[0101] 作为对安全散列的添加，可以视需要包括第二秘密加密密钥，并将其添加至上文针对金融交易详情的项目列表中，并因此将其包括在该散列函数的计算中。该额外秘密值也将用金融组织的安全计算模块200上的其他密钥材料来存储。虽然密钥散列被认为是安全的，但密码破译者和黑客在破解散列和其他加密过程中不断取得进展。为了保持本发明的实施例更加安全，可以在散列函数中包括第二秘密密钥，从而以对安全计算模块200而言容易处理的方式来增加计算安全散列的熵。

[0102] TNI是与当前交易和安全计算模块200相关的唯一数字。该唯一数字可以若干方式来产生。作为非限制性实例，TNI可以仅为通过安全计算模块200执行的交易的运行递增计数。作为另一个非限制性实例，只要安全计算模块200和用户的金融组织300可产生用于当前交易的相同号码，则TNI可以通过诸如伪随机产生号码之类的复杂算法来产生。

[0103] 因此，TNI涉及用于具体交易给定方(例如，买方或卖方)的计数或计算的交易号码，并且是在交易签署时产生。买方和卖方可以具有不同的交易号码，因为他们将会执行不同数量的交易或使用不同的TNI产生算法。在其他实施例中，对于买方和卖方而言，TNI可以相同。在此情况下，TMI将由发起交易(买方或卖方)的一方来计算，并且将用于另一方的数字签名过程中。

[0104] 将TNI包括在金融购买包签署计算中作为金融交易详情的一部分。TNI还连同签署的FPP一起发送至金融组织以协助索引购买交易。因此，当买方签署FPP时该买方使用的TNI很可能不同于当卖方签署FPP时该卖方使用的TNI。

[0105] 应注意，连同买方的安全数字签名和卖方的安全数字签名一起的金融交易详情可以经由近场无线通信通道245在买方的安全计算模块200A与卖方的安全计算模块200B之间转移。近场通信无线通道245可以具有默认频率和协议。作为非限制性实例，该近场通信通道245可以为RFID。然而，如果默认通道不可用，则可以使用另一个通道，或者用户选择不同的通道来使用。作为非限制性实例，其他可能的通信通道是短消息服务(SMS)、多媒体消息服务(MMS)、无线应用协议(WAP)、蓝牙、WiFi以及其他适当的协议。

[0106] 在一些情况下，近场无线通信通道245可能由于其他人的窥探而不是特别安全。然而，本发明的实施例通过使用买方和卖方两者的安全数字签名来确保不泄密当前交易。另一方面，如果未加密，则金融交易详情可能是可被发现的，从而如果在金融交易详情中存在足够的信息，则可能导致身份盗窃。因而，一些实施例可以包括金融购买包的加密和解密。另外，在一些实施例中，受控内容可以是加密的。

[0107] 加密和解密可以使用任何适当的密码算法。作为非限制性实例，密码算法可以是本领域众所周知的诸如高级加密标准(AES)的对称算法。对称密码术要求秘密密钥仅为加密者和解密者所知。因此，该加密的进行可使得秘密密钥为用户和该用户的金融组织所知。在此情况下，该秘密密钥可以是通过使用散列算法用于产生安全数字签名的相同密钥，或其可以是用于加密/解密的不同秘密密钥。或者，如下文所阐述，该秘密密钥可以是买方与卖方之间在发现过程期间确定的秘密密钥。

[0108] 作为另一个非限制性实例，该密码算法可以是本领域众所周知的诸如RSA的不对称算法。RSA表示首先公开该加密算法的个人的首字母。在不对称密码术中，使用公共密钥和私人密钥两个密钥。用户可以让任何人知道其公共密钥，而使私人密钥仅为其自己所知。希望向该用户发送已加密消息的任何人通过使用该用户的公共密钥来对消息加密。一旦加密，则该消息仅可通过仅为用户所知的私人密钥来解密。

[0109] 因此，可以存在通过安全计算模块200来存储和管理的若干密钥，诸如，秘密数字签名密钥、秘密加密密钥、私人密钥以及公共密钥。通常，用户不直接更新其加密密钥和签署密钥。换句话说，用户有权使用其密钥，但无权操纵其密钥。密钥的更新、添加、或改变可以通过控制服务器的制作安全计算模块200的组织来完成。

[0110] 为安全地管理和更新密钥，可以将个人识别码(PIC)例程包括在安全计算模块200中，以允许用户向安全计算模块200认证其本人。PIC可以包括仅为用户和安全计算模块200所知的一系列字母数字值。在另一实施例中，PIC可以是诸如指纹或视网膜扫描的一些生物测定特征的数字表示。在另一实施例中，用户可以发起PIC输入请求，其中安全计算模块200输出一系列字母数字的字符，用户必须依次重新输入或重新键入这些字符并且将其提交回安全计算模块200。当然，PIC例程可以包括组合输入生物测定信息和字母数字值。此外，PIC例程可以包括用于用户进入的随机全自动区分计算机和人类的图灵测试(CAPTCHA)算法。CAPTCHA是显示的倾斜且扭曲的模糊字符，这些字符人类可辨别，但计算机可能不能辨别。

[0111] 在其他实施例中，安全计算模块200可以直接从连接或可连接的输入装置(未示出)处接收PIC输入。该输入装置的一个实例为经由导线直接连接入安全计算模块200中的外部的指纹或视网膜扫描读出器装置。此额外硬件提供更安全的输入，其不要求这些输入经过主机装置110的存储器506或处理器502或经过包含安全计算模块200的其他计算装置。

[0112] 用于加密/解密以及用于安全散列产生数字签名的秘密密钥可以在安全计算模块200为了交易处理而连接至金融组织时，由该金融组织周期性地刷新。如果如此配置，则金融组织300可以视需要为了重新键入而发起至包括安全计算模块200的主机装置110的连接。

[0113] 作为所用密钥的非限制性实例，可以为各安全计算模块200产生两个公共和私人密钥对。对于第一密钥对来说，公共密钥是存储在用户的安全计算模块200中，而私人密钥则是用金融组织的安全计算模块200来存储。该第一密钥对允许用户的安全计算模块200对将发送至金融组织的信息进行加密。对于第二密钥对来说，私人密钥是存储在用户的安全计算模块200中，而公共密钥则是用金融组织的安全计算模块200来存储。该第二密钥对允许金融组织的安全计算模块200对将发送至用户的安全计算模块200的信息进行加密。可以使用这两个密钥对系统，以便各用户的安全计算模块200都可以具有用来与金融组织通信的其自身唯一的加密通信通道。为此，具有分离的密钥可保护免于这样一种情况出现：如果

一个加密通道被破解，则所有加密通道将被破解。另外，由于公共密钥加密比对称密钥加密缓慢许多，所以这两个密钥对可以用于交换可用于具体交易的临时对称密钥。

[0114] 受控内容的分发可以用某些分发规则和使用规则来进行。分发规则规定内容可以如何分发。举例而言，可以将分发规定为无限制分发。在另一个实例中，可以将分发规定为超过某个量后就不允许进一步分发。在另一个实例中，可以将分发限定于规定的时间周期、具体时间、或选定的日期中。

[0115] 在另一个实例中，可以将分发限定于某些分发群体。换句话说，可将分发限定于具有规定群体成员资格的个体。作为非限制性实例，这允许大学教授将课本或测试稿分发给当前班级，并且仅分发给当前班级而不会分发给公众。这还允许公司将“专有的”材料仅分发给其雇员，而不会分发给整个社会。可以将分发群体名称维持在安全计算模块200上，并且也可在交易期间用分发群体的中央储存库来对其进行验证。

[0116] 在访问授权令牌的情况下，分发可以包括从内容所有者(诸如，场馆业主、入场券分销商、或其他适当的活动入场券卖方)处分发。另外，当有授权时，分发可以在个体之间进行。以此个体方式，可以将访问授权令牌的分发比作受控制的入场券转售市场。

[0117] 在本发明的实施例中，当分发了内容所有者的受控内容时，内容所有者可以在财政上得到补偿。作为非限制性实例，版税费可预设为某个量或者可定期确定。定期版税可以允许内容所有者根据市场或其他影响力的指导来提高或降低购买价格和版税费。举例而言，当由内容所有者或内容供应商350降低了并未在售的受控内容的价格时，该受控内容可能更畅销。相反地，内容所有者可能希望提高畅销的受控内容价格。动态定价还允许“特价日”或期望折扣的其他时间。

[0118] 另外，本发明的实施例允许内容由先前的买方转售。在转售过程中，内容所有者可以征收针对从转售方至买方的额外分发的版税。另外，如果分发规则允许，则转售方可以为自己征收费用，同时也确保将规定版税费付给内容所有者。如果分发规则允许，则转售方与买方之间可以协商该转售方费用。

[0119] 在一些实施例中，可以为预定时间段设置转移限制和分发规则。此外，可以将买方对受控内容的访问限定于预定时间段。在该预定时间段之后，安全计算模块可以通过删除、不解密、不允许访问、或其组合来阻止对受控内容的访问。

[0120] 在一些实施例中，安全计算模块200可以解密该受控内容并且将其转移至主机装置110以供使用。在其他实施例中，安全计算模块200可以将受控内容保留在安全计算模块200的存储器230中，并且根据需要将其提供给主机装置110。

[0121] 为了在两个个体之间用无线通信装置来执行金融交易或受控内容分发，安全计算模块200执行发现过程，以使得两个安全计算模块200彼此觉察。当使用便携式电子装置时，该发现过程经由近场无线通信通道(245B-245D)中的一个通道来进行。

[0122] 在无线发现过程中，从具有安全计算模块200的主机装置110中进行公开的用户选择以发起交易并且连接至另一个主机装置110。该过程通常不像对大多数RFID支付卡和装置而言那样简单的“自动”进行，因为RFID过程可能固有地不安全并且易于盗窃、窃取和滥用。然而，在一些实施例中，与传统RFID系统的反向兼容性可以经启用来授权自动响应。作为非限制性实例，可以切换该用途以启用针对诸如地铁费用交易之类低价交易的项目的自动响应。作为另一个非限制性实例，传统RFID系统可以用于将访问授权令牌从安全计算模

块200传达至准入控制器(未示出)。可以通过场馆来操作该准入控制器,以允许通过准入控制器从一或多个安全计算模块接收的场馆访问授权令牌的准入。

[0123] 发现过程可以使用由探究过程用来寻找兼容装置的本行业众所周知的若干方法中的任何方法。当发现此类装置时,双方可以输入或协商相同的秘密会话密钥值等。然后,可以基于该共享的秘密密钥值来进行会话加密。该发现和密钥协商过程的非限制性实例是本领域众所周知的蓝牙®配对和蓝牙®配对过程的增强。

[0124] 发现过程可以经由包含在安全计算模块200之内的近场无线通信机240来进行。使安全处理器来控制信息发送和接收的内容、时间和方式可以增强系统安全性。

[0125] 视需要,可以使用传统的在线客户-服务器方法、或者诸如安全短消息服务(SMS)协议之类的存储和转发格式来进行该发现过程。

[0126] 图6为图示在从内容供应商350处分发和购买受控内容期间可执行的过程600的简化程序框图。可以参考图6,并且有时可以参考图4和图5来进行过程600。应注意,在过程600期间在实体之间进行的任何通信可以如上文所阐述那样加密或不加密。

[0127] 以在操作块612处买方通过网络从内容供应商350处选择受控内容来开始过程600。内容供应商350可以是各种在线分销商,诸如,iTunes、Amazon.com、Wal-Mart在线等。另外,内容供应商350可以是实体商店,诸如Wal-Mart当地商店、Best Buy当地商店等。内容供应商350还可以是当地商店或其他设施中的分发亭。在过程600中,内容供应商350还可以称为卖方350。

[0128] 在操作块614中,将交易详情、卖方的凭证以及卖方的数字签名从卖方350传达至买方的安全计算模块200A。连同该交易的金融信息一起,交易详情可以包括关于内容所有者、内容所有者的金融组织以及针对该受控内容的分发规则的信息。

[0129] 在操作块616中,在主机装置110A上为买方呈现对话框,该对话框指示交易详情、分发规则以及其他相关信息。提示买方接受或拒绝该交易。如果拒绝交易,则过程600停止(未示出)。如果接受交易,则买方产生包括关于该内容的交易详情、分发规则以及其他信息的金融购买包,并且产生买方的安全数字签名。然后,买方将该金融购买包发送回卖方350。

[0130] 如果卖方或买方没有批准并且数字地签署FPP,则该过程停止(未示出)。如果要继续交易,买方或卖方可以将金融购买包发送至金融组织。

[0131] 判定块620确定卖方是否要传达FPP。如果卖方传达该金融购买包,则操作块622指示卖方将FPP发送至卖方的金融组织300B。在操作块624中,卖方的金融组织300B通过检查卖方的安全数字签名来认证卖方。

[0132] 该认证过程使用卖方的秘密密钥在卖方的数字签名上执行反向散列过程,并且确定交易详情是否准确,交易号码标识符是否正确,以及卖方的凭证是否使卖方的账户与该金融组织匹配。

[0133] 然后,卖方的金融组织300B可以批准或拒绝该交易。如果拒绝,则卖方的金融组织300B将消息发送回卖方,并且交易终止(未示出)。如果批准,则卖方的金融组织300B通过网络150将FPP和许可发送至买方的金融组织300A。在一些情况下,买方的金融组织300A和卖方的金融组织300B可以是相同的实体,且可能不需要通过网络150“发送”FPP。

[0134] 在操作块626中,以类似于上述卖方认证过程的方式,买方的金融组织300A通过使用买方的秘密密钥检查买方的安全数字签名来认证买方。然后,买方的金融组织300A可以

批准或拒绝交易。如果拒绝，则买方的金融组织300A将消息发送至买方的主机装置110A，并且交易终止（未示出）。如果批准，则买方的金融组织300A将资金转移至卖方的金融组织300B。

[0135] 返回判定块620，如果买方传达金融购买包，则操作块632指示买方经由网络150将FPP发送至买方的金融组织300A。在操作块634中，买方的金融组织300A如上文所阐述那样通过使用买方的秘密密钥检查买方的安全数字签名来认证买方。

[0136] 然后，买方的金融组织300A可以批准或拒绝交易。如果拒绝，则买方的金融组织300A将消息发送回买方的主机装置110A，并且交易终止（未示出）。如果批准，则买方的金融组织300A通过网络150将FPP和许可发送至卖方的金融组织300B。在一些情况下，买方的金融组织300A和卖方的金融组织300B可以是相同的实体，且可能可以不需要通过网络150“发送”FPP。

[0137] 在操作块636中，卖方的金融组织300B如上文所阐述那样通过使用卖方的秘密密钥检查卖方的安全数字签名来认证卖方。然后，卖方的金融组织300B可以批准或拒绝该交易。如果拒绝，则卖方的金融组织300B将消息发送至卖方350，并且交易终止（未示出）。如果批准，则卖方的金融组织300B将许可发送回买方的金融组织300A。在操作块638中，买方的金融组织300A将资金转移至卖方的金融组织300B。此时在该过程中，金融交易已完成。

[0138] 判定块640确定是否应将交易结果通知卖方。如果是的话，则在操作块642中，卖方的金融组织300B将交易结果发送至卖方350。

[0139] 判定块644确定是否应将交易结果通知买方。如果是的话，则在操作块646中，买方的金融组织300A将交易结果发送至买方的安全计算模块200A。

[0140] 过程块648指示受控内容从卖方350传达至买方的安全计算模块200A。如先前所示，安全计算模块可以在需要时解密受控内容，并且将受控内容存储在安全计算模块200A上的存储器230中或将其转移至主机装置110A。

[0141] 在过程600中，买方的安全计算模块200A、卖方350、买方的金融组织300A以及卖方的金融组织300B中的任何一者都可以保留一份关于该金融交易和其成功或其由于任何一方未批准而失败或其由于资金不足而失败的日志。

[0142] 在过程600中，一些通信可以经由诸如互联网的中间通信网络来进行，一些通信可以经由蜂窝通信通道来进行，并且一些通信可以经由近场无线通信通道来进行。

[0143] 金融组织300包括安全计算模块200，并且可以采用企业版的安全计算模块200软件、硬件、或其组合。该企业版产生对于许多连续且同时的交易而言更稳健的安全机制。为确保交易之间额外的安全性，该用于安全计算模块200的企业软件可以将个体交易间的动态交易存储器归零。

[0144] 图7A和图7B是图示在个体之间分发和购买受控内容期间可执行的过程700的简化程序框图。可以参考图7A和图7B，并且有时可以参考图4和图5来进行过程700。应注意，在过程700期间在实体之间进行的任何通信可以如上文所阐述那样加密或不加密。

[0145] 以在操作块702处转售方产生交易详情来开始过程700。连同交易的金融信息一起，所述交易详情可以包括关于内容所有者、内容所有者的金融组织以及针对该受控内容的分发规则的信息。将交易详情、卖方的凭证以及卖方的数字签名从转售方的安全计算模块200B传达至买方的安全计算模块200A。

[0146] 在操作块704中，在主机装置110B上为买方呈现对话框，该对话框指示交易详情、分发规则以及其他相关信息。提示买方接受或拒绝该交易。如果拒绝交易，则过程700停止(未示出)。如果接受交易，则买方的安全计算模块200B产生包括关于该内容的交易详情、分发规则以及其他信息的金融购买包，并且产生买方的安全数字签名。然后，买方将该金融购买包发送回转售方的安全计算模块200A。

[0147] 如果转售方或买方没有批准并且数字地签署FPP，则该过程停止(未示出)。在操作块708中，转售方的安全计算模块200A将金融购买包发送至内容所有者的金融组织300B和买方的金融组织300A。

[0148] 在操作块710中，内容所有者的金融组织300B验证交易详情、转售方的分发授权以及分发规则。在一些情况下，内容所有者的金融组织300B可能不知道转售方的分发授权或分发规则的详情。在那些情况下，内容所有者的金融组织300B可以经由网络150与内容所有者或内容供应商350通信以验证转售方的分发授权和分发规则。如果验证了交易详情与任何内容规则和授权，则内容所有者的金融组织300B可以批准交易。否则，内容所有者的金融组织300B可以拒绝交易。然后，内容所有者的金融组织将许可或拒绝发送至买方的金融组织300A。

[0149] 在操作块712中，买方的金融组织300A如上文所阐述那样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交易详情和认证买方。

[0150] 然后，买方的金融组织300A可以批准或拒绝交易。如果拒绝，则买方的金融组织300A将消息发送至买方的主机装置110A，并且交易终止(未示出)。如果批准，则买方的金融组织300A将资金转移至内容所有者的金融组织300B。

[0151] 参见图7B，在判定块714中，该过程确定转售方是否有资格接收针对转售受控内容的费用。如果没有，则控制往下传至判定块724。

[0152] 如果转售方将接收费用，则在操作块718中，转售方将FPP发送至转售方的金融组织(未示出，可考虑为图5中的第三金融组织300)。

[0153] 在操作块720中，转售方的金融组织300如上文所阐述那样通过使用转售方的秘密密钥检查转售方的安全数字签名来认证转售方。然后，转售方的金融组织300可以批准或拒绝交易。如果拒绝，则转售方的金融组织300将消息发送回转售方的主机装置110A，并且交易终止(未示出)。如果批准，则转售方的金融组织300通过网络150将FPP和许可发送至买方的金融组织300A。在一些情况下，买方的金融组织300A和转售方的金融组织300可以是相同的实体，且可能不需要通过网络150“发送”FPP。

[0154] 在操作块722中，买方的金融组织300A将针对转售方的费用的资金转移至转售方的金融组织300。此时在该过程中，金融交易已完成。

[0155] 判定块724确定是否应将交易结果通知转售方。如果是的话，则在操作块726中，转售方的金融组织300将交易结果发送至转售方的安全计算模块200A。

[0156] 判定块728确定是否应将交易结果通知内容所有者、内容供应商350、或其组合。如果是的话，则在操作块730中，内容所有者的金融组织300B将交易结果发送至内容供应商350。

[0157] 判定块732确定是否应将交易结果通知买方。如果是的话，则在操作块734中，买方的金融组织300A将交易结果发送至买方的安全计算模块200A。

[0158] 过程块648指示受控内容从转售方的安全计算模块200A传达至买方的安全计算模块200B。如先前所示，安全计算模块可以在需要时解密受控内容，并且将受控内容存储在安全计算模块200B上的存储器230中或将其转移至主机装置110B。

[0159] 在过程700中，买方的安全计算模块200B、转售方的计算模块200A、买方的金融组织300B、转售方的金融组织300以及内容供应商的金融组织300A中的任何一者都可以保留一份关于该金融交易和其成功或其由于任何一方未批准而失败或其由于资金不足而失败的日志。

[0160] 在过程700中，一些通信可以经由诸如互联网的中间通信网络来进行，一些通信可以经由蜂窝通信通道来进行，并且一些通信可以经由近场无线通信通道来进行。

[0161] 金融组织300包括安全计算模块200，并且可以采用企业版的安全计算模块200软件，该企业版的安全计算模块200软件产生对于许多连续且同时的交易而言更稳健的安全机制。为确保交易之间额外的安全性，该用于安全计算模块200的企业软件可以将个体交易间的动态交易存储器归零。

[0162] 虽然已参考具体实施例描述了本发明，但本发明不限于这些所述实施例。相反，本发明仅受所附权利要求书的限制，该所附权利要求书在其范围内包括根据所描述的本发明的原理来操作的所有等效的装置或方法。

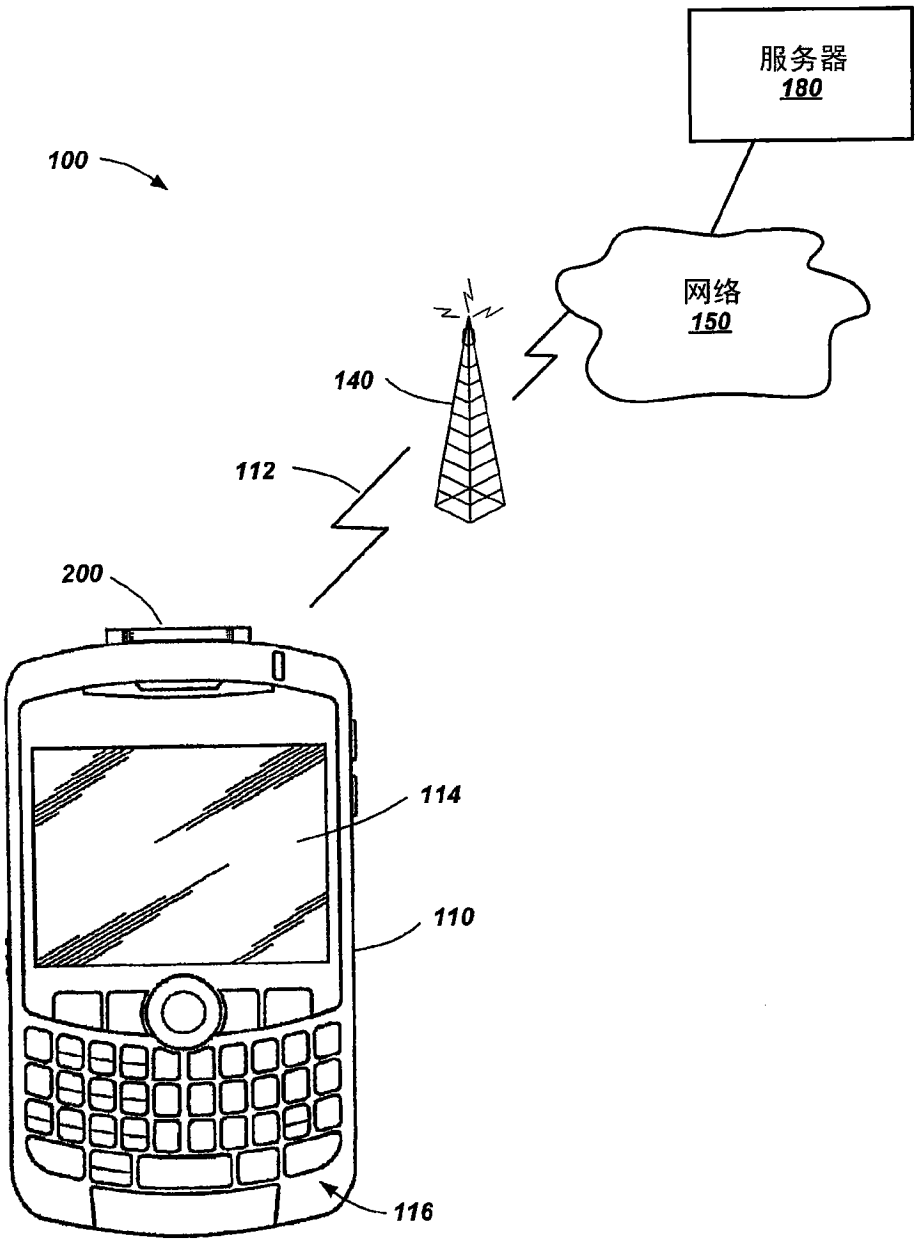


图1

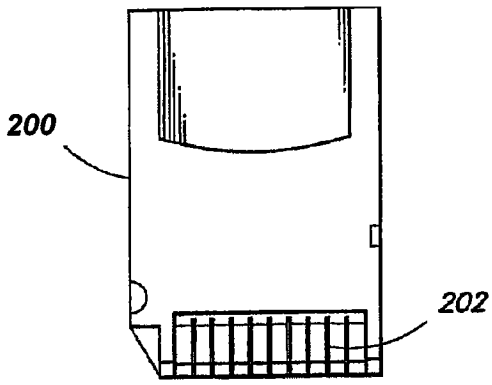


图2

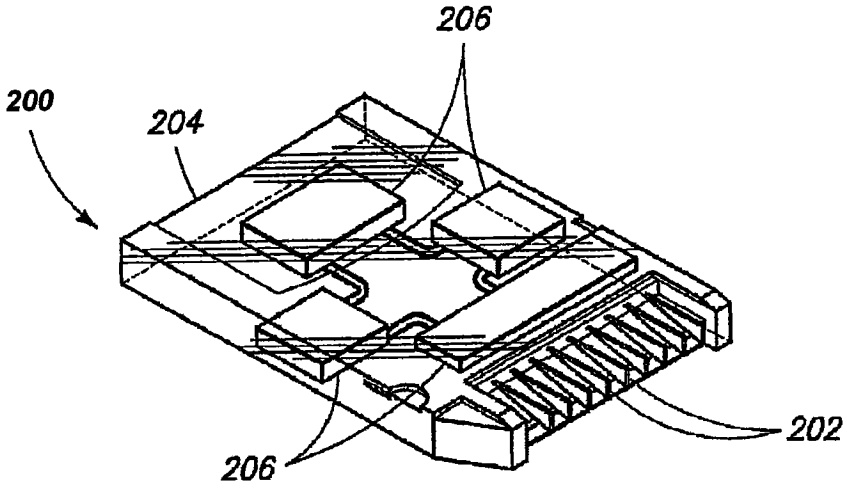


图2A

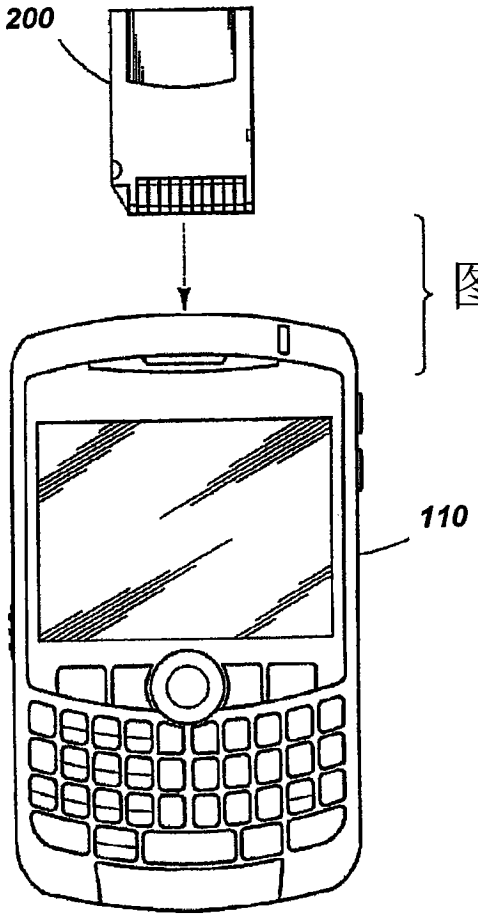


图 3

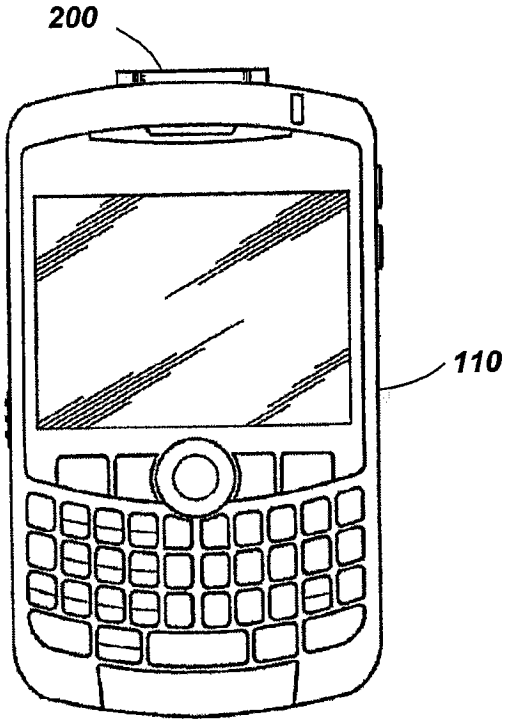


图 3A

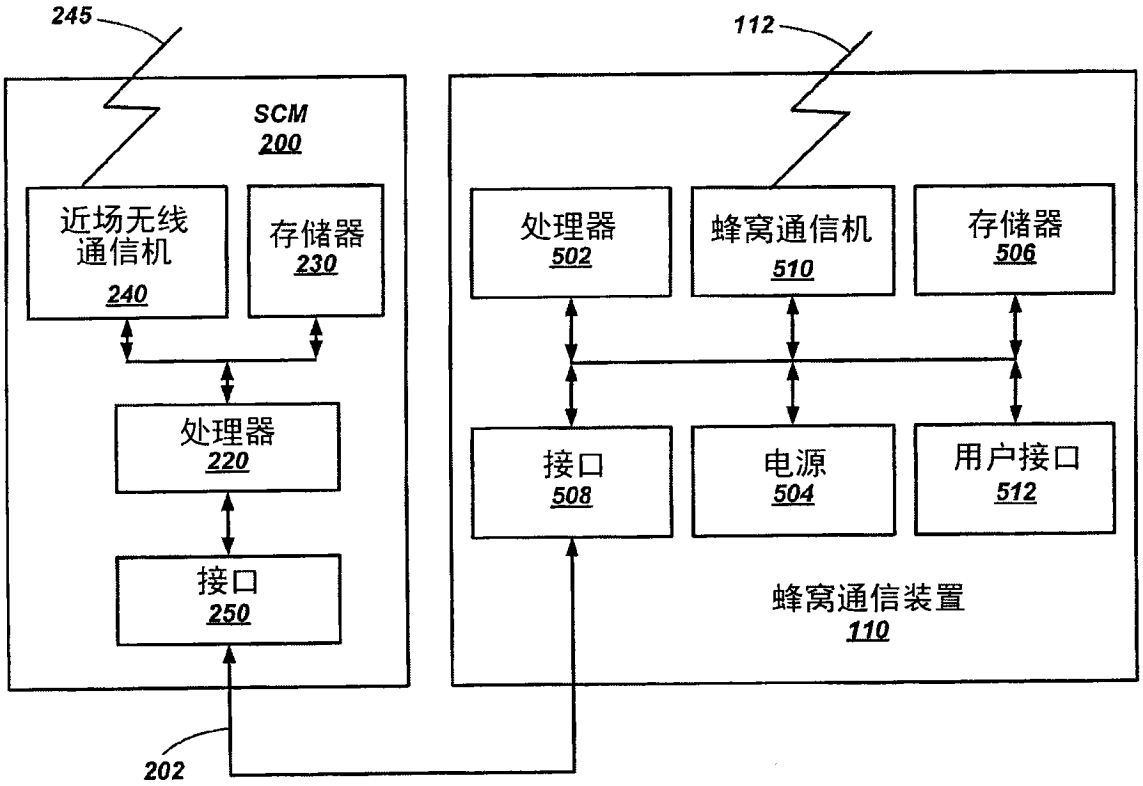

245
SCM
200
近场无线通信机
240
存储器
230
处理器
220
接口
250
202
112
处理器
502
蜂窝通信机
510
存储器
506
接口
508
电源
504
用户接口
512
蜂窝通信装置
110

图4

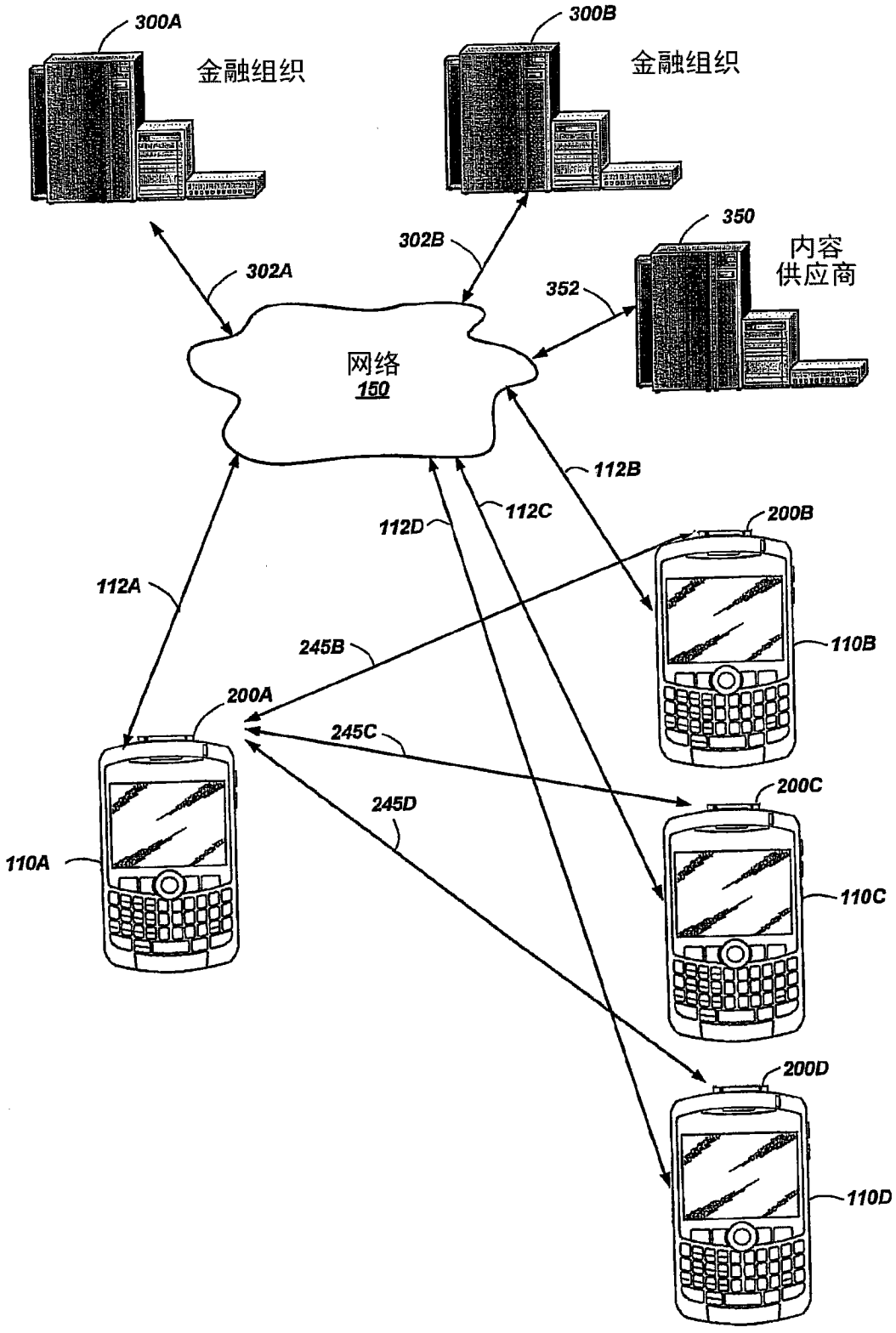

300A
金融组织
300B
金融组织
350
内容
供应商
302B
302A
352
网络
150
112B
112D
112C
200B
112A
110B
245B
200A
245C
200C
245D
110A
110C
200D
110D

图5

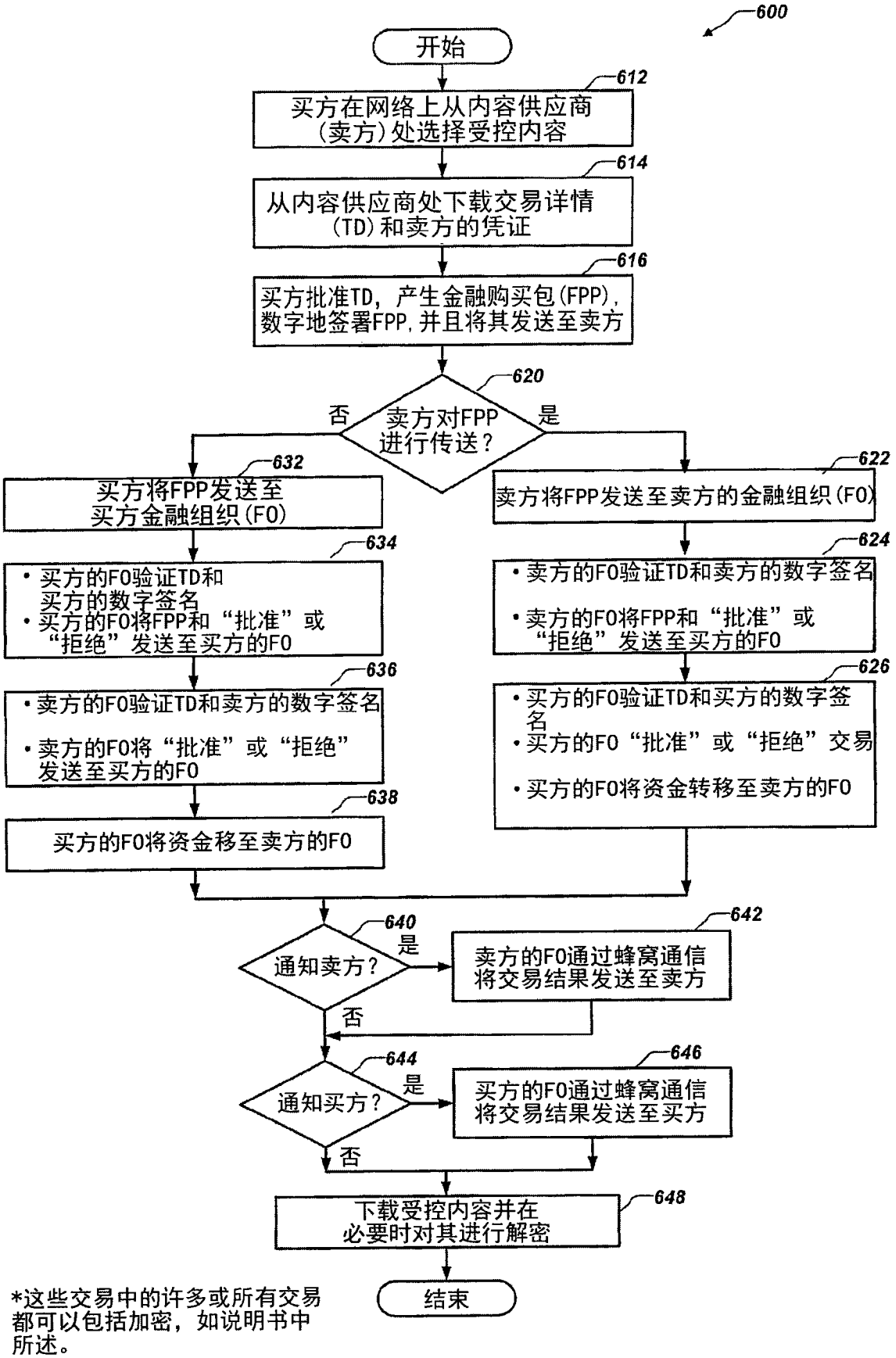
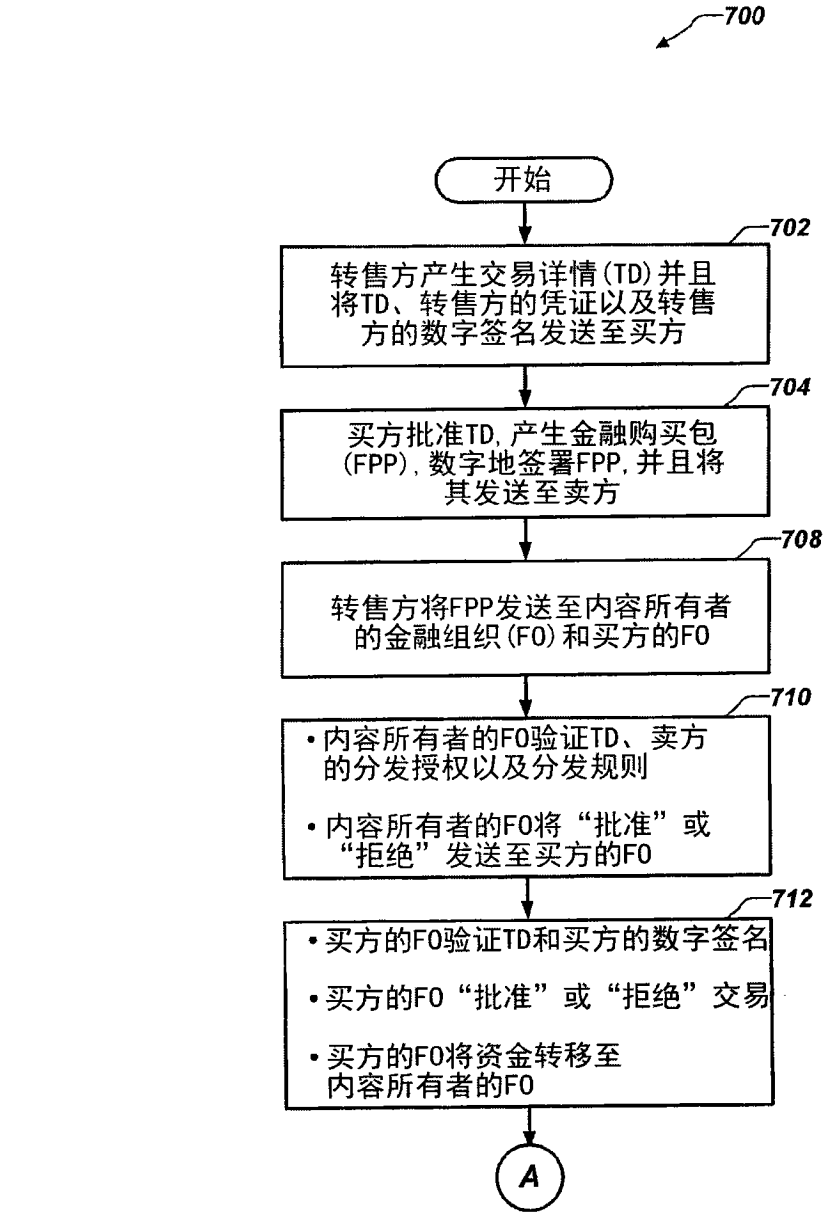

600
开始
612
买方在网络上从内容供应商(卖方)处选择受控内容
614
从内容供应商处下载交易详情(TD)和卖方的凭证
616
买方批准TD，产生金融购买包(FPP)，数字地签署FPP，并且将其发送至卖方
620
卖方对FPP进行传送？
否
是
632
买方将FPP发送至买方金融组织(FO)
634
• 买方的FO验证TD和买方的数字签名
• 买方的FO将FPP和“批准”或“拒绝”发送至买方的FO
636
• 卖方的FO验证TD和卖方的数字签名
• 卖方的FO将“批准”或“拒绝”发送至买方的FO
638
买方的FO将资金移至卖方的FO
622
卖方将FPP发送至卖方的金融组织(FO)
624
• 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”发送至买方的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将资金转移至卖方的FO
640
通知卖方？
是
642
卖方的FO通过蜂窝通信将交易结果发送至卖方
否
644
通知买方？
是
646
买方的FO通过蜂窝通信将交易结果发送至买方
否
648
下载受控内容并在必要时对其进行解密
结束
*这些交易中的许多或所有交易都可以包括加密，如说明书中所述。

图6



*这些交易中的许多或所有交易都可以包括加密，如说明书中所述。

图7A

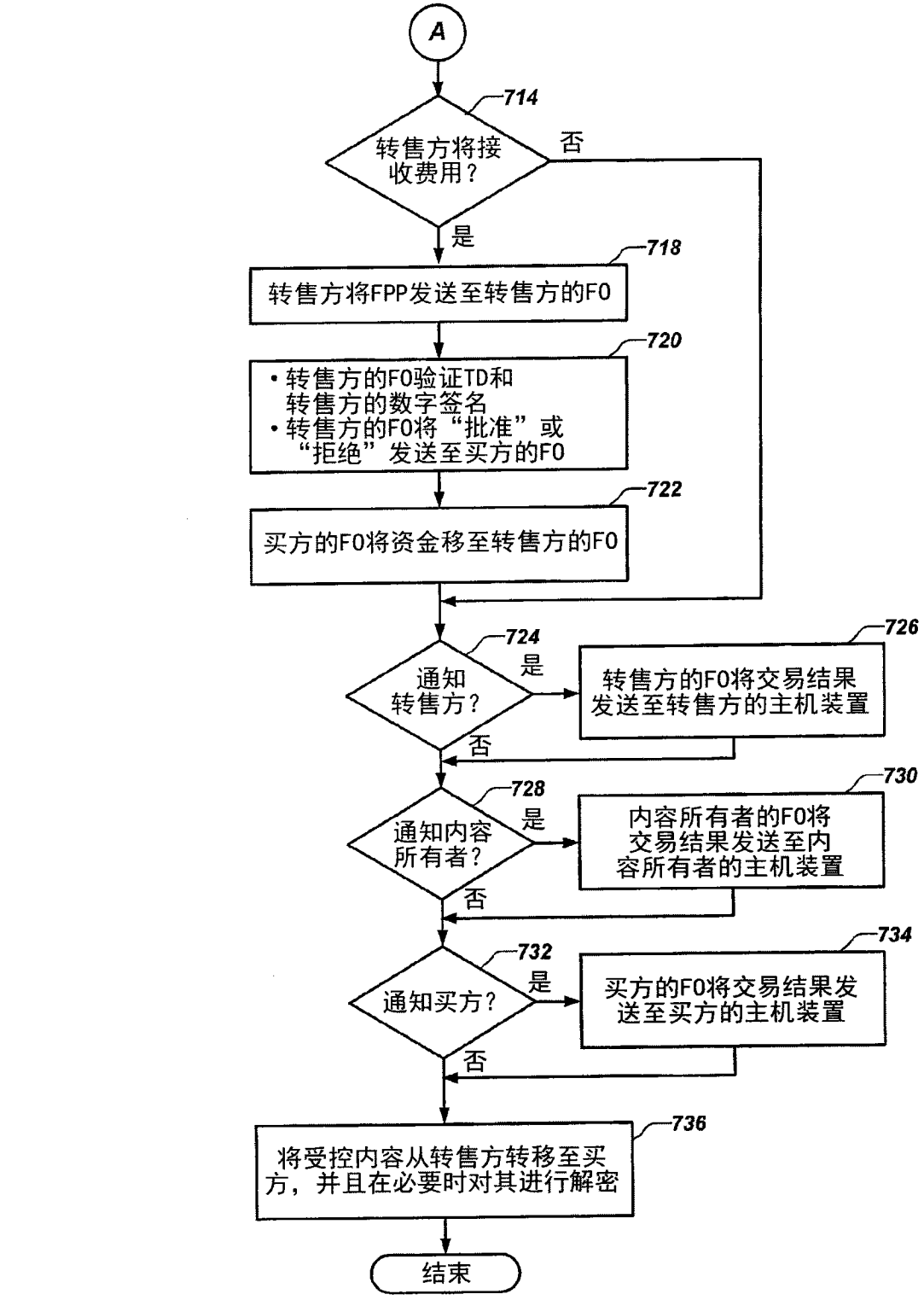

A
714
转售方将接收费用？
否
是
718
转售方将FPP发送至转售方的FO
720
• 转售方的FO验证TD和转售方的数字签名
• 转售方的FO将“批准”或“拒绝”发送至买方的FO
722
买方的FO将资金移至转售方的FO
724
通知转售方？
是
726
转售方的FO将交易结果发送至转售方的主机装置
否
728
通知内容所有者？
是
730
内容所有者的FO将交易结果发送至内容所有者的主机装置
否
732
通知买方？
是
734
买方的FO将交易结果发送至买方的主机装置
否
736
将受控内容从转售方转移至买方，并且在必要时对其进行解密
结束
*这些交易中的许多或所有交易都可以包括加密，如说明书中所述

图7B