[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32

# [12] 发明专利说明书

[21] ZL 专利号 99816175.6

[45] 授权公告日 2004 年 8 月 4 日

[11] 授权公告号 CN 1160902C

[22] 申请日 1999.12.15 [21] 申请号 99816175.6
[30] 优先权
[32] 1998.12.16 [33] FI [31] 982728
[86] 国际申请 PCT/FI1999/001036 1999.12.15
[87] 国际公布 WO2000/039958 英 2000.7.6
[85] 进入国家阶段日期 2001.8.14
[71] 专利权人 斯麦脱信托有限公司
地址 芬兰束那拉
[72] 发明人 H·瓦它嫩
审查员 朱少华

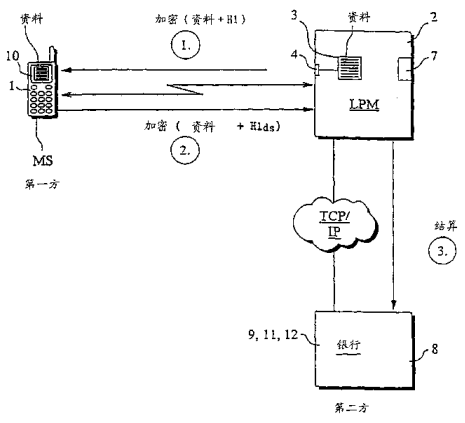
[74] 专利代理机构 上海专利商标事务所
代理人 钱慰民

权利要求书 2 页 说明书 7 页 附图 4 页

[54] 发明名称 实现数字签名的方法和系统

[57] 摘要

一种用移动站按保密方式对电子表格数字签名的方法。 在该方法中，向移动站传递待签资料，其中待签资料包括表格、表格标识符、共享信息和/或表格所加实质信息。 根据资料计算出第一散列码(H1)。 将散列码加至资料，以传递给移动站。用移动站对传递给移动站的资料数字签名。 通过对经签名的散列码与签名前根据资料计算得到的散列码作比较验证经签名的被传资料的可靠性。 由于本发明，在各种应用中可以安全地使用移动站进行数字签名。




ISSN1008-4274

1. 一种利用移动站按保密方式对电子表格数字签名的方法，所述方法包括以下步骤：

将待签资料传递给移动站，所述资料包括表格、表格标识符、共享信息和/或对表格所加的实质信息，其特征在于，

由待签资料计算出第一散列码(H1)；

将第一散列码加至所述资料中，以便传递给所述移动站；

用移动站对传递给移动站的资料数字签名；

将经签字的散列码与签名前由资料计算出的第一散列码作比较，验证经签名的被传资料的可靠性。

2. 如权利要求 1 所述的方法，其特征在于，根据表格标识符和与表格相关的实质信息生成待签资料。

3. 如权利要求 2 所述的方法，其特征在于，最好在向移动站传递资料之前根据待签资料计算出第一散列码。

4. 如权利要求 1 所述的方法，其特征在于，

将传递给移动站进行签名的资料传递给第二方；并且

将经签名的资料也传递给第二方，第二方验证签名的可靠性。

5. 如权利要求 1 所述的方法，其特征在于，

在移动站和第二方之间作传递之前对资料加密，并且

在对资料作诸如签名和可靠性验证等任何处理之前对加密资料解密。

6. 如权利要求 1 所述的方法，其特征在于，

用预先同意的且配备了标识符的表格模板生成所述表格，在传递给移动站之前将实质信息填入表格模板中。

7. 如权利要求 1 所述的方法，其特征在于，

用一散列函数生成所述第一散列码。

8. 如权利要求 1 所述的方法，其特征在于，

用公开和私人密钥方法对消息签名和/或加密。

9. 如权利要求 1 所述的方法，其特征在于，

在对资料签名之前，将资料和/或其一部分呈现在移动站中。

10. 如权利要求 1 所述的方法，其特征在于，

在将资料传递到移动站之前，以签名模式起动移动站。

11. 如权利要求 1 所述的方法，其特征在于，

对资料盖时间戳，并且

在签名认证后将资料的签名事务归档。

12. 一种利用移动站(MS)按保密方式对电子表格数字签名的系统，所述系统包括：

付费机(2)；

与付费机相连、用于生成待签资料的装置(3)，所述资料包括表格、表格标识符、共享数据和/或对表格所加的实质信息；

与付费机相连、用于向移动站(MS)传递资料的装置(4)；其特征在于，

所述付费机包括用于根据待签资料计算第一散列码(H1)的装置(5)；

所述移动站包括用于对传递给它的资料签名的签名装置(6)；

所述付费机包括通过对经签名散列码($H1_{ds}$)与签名前根据资料计算得的散列码(H1)作比较来验证经签名的被传资料之可靠性的装置(7)。

13. 如权利要求 12 所述的系统，其特征在于，所述系统包括：

服务器(8)，它与付费机(2)和移动站(MS)相连，并由第三方控制；并且

所述移动站包括对签名资料加密的装置。

14. 如权利要求 12 所述的系统，其特征在于，服务器(8)包括：

用于验证数字签名可靠性的装置(9)。

15. 如权利要求 12 所述的系统，其特征在于，所述移动站包括：

在对资料签名之前将资料和/或其一部分呈现在移动站中的装置(10)。

16. 如权利要求 12 所述的系统，其特征在于，所述服务器(8)包括

对资料盖时间戳的装置(11)，和

在签名认证后将资料之签名事务归档的装置(12)。

# 实现数字签名的方法和系统

本发明涉及一种电信系统和一种数字信息的签字加密技术。本发明尤其涉及一种可以对电子表格或其它电子信息签字并验证签名及签名人可靠性的系统。

## 发明背景

在现有技术中，用数字移动站，例如“全球移动通信系统”(GSM)系统中的移动站，进行商业交易已为人知，比如用电子手段支付帐单或付费等。专利申请 US 5,221,838 披露了一种付费用的装置。在该说明书描述的电子付费系统中，能够进行有线和/或无线数据传输的终端设备被用作付费终端，终端设备包括输入信息用的阅卡机、小键盘和条形码阅读器，以及用于呈现付款信息的显示单元。

专利说明书 WO 94/11849 揭示了一种通过移动电话系统来利用电信服务并进行付费的方法，其中描述了一种终端设备，它通过电信系统与包含服务提供者付费系统的服务提供者主计算机进行通信。在移动电话网中使用的终端设备(即移动站)可以配备用户标识模块，该模块包括用于识别用户并加密电信的用户信息。用户信息可以读入终端设备，在移动站中使用。说明书以 GSM 系统为例，将 SIM 卡(SIM，用户标识模块)用作用户识别单元。

在 WO 94/11849 的系统中，移动站与移动电话网中的基站通信。依照该说明书，还与支费系统建立连接，将待付金额以及识别用户所需的数据传递给付费系统。在该说明书所描述的银行业务中，客户将银行提供的、包含 SIM 单元的服务卡放入 GSM 网的终端设备中。在基于电话的银行业务中，终端设备可以是符合标准的 GSM 移动站。利用此说明书中的方法，可以用无线电信连接付费和/或支付帐单，或者实现其它银行或现金业务。

上述方案的问题在于，从付费者和收费者的角度来说，它们没有考虑付费的可靠性。当用移动站付费时，付费和收费双方信任付费系统是很重要的。付费者必须确切知道他正在付什么费、付多少、付给谁、如何付等等。收费者也必须确切知道谁在付费、付什么费、付了多少等等。

众所周知，将电子表格的信息从一处发至另一处是很容易的。但要保证所传信息在传输中不变以及例如移动站显示器上呈现的信息以真正相同表格不变地发送给接收方就会困难一些。

早先已知的作法是使用散列码，这是一种根据待发信息形成并计算出的数据字段。计算散列码的一般算法是一种单向函数，换句话说，不能对散列码解密，以揭示生成该码的信息。可用于此目的的一种算法是 SHA-1(保密散列算法)。

数字签名是电子付费的一般要求，用于验证所发资料的完整性和原发送方。数字签名是用发送方密钥对根据待发资料计算出的散列码进行加密而生成的。由于他人不知道发送方密钥，所以对加密资料解密的接收方得到下述保证，即该资料是由所述发送方生成的，并且没有改变。数字签名所用算法的一个例子是 RSA 加密算法，这是一种根据私人密钥和公开密钥的加密系统，也可用于对消息加密。

发明目的

本发明的目的是解决上述问题。本发明的一个具体目的是，提供一种用移动站对一种表格或相应信息签字的新型方法和系统。在本文中，“表格”可以指具有各种内容的多种类型的消息、专电或信息结构。表格可以由对象型或软件对象型信息组成，它们都可以按电子表格进行处理。

本发明的另一个目的是，揭示一种实现商业交易的简单方法，诸如利用移动站支付帐单和与银行交易等，这是一种用本发明技术很容易实现的方法。

发明内容

本发明涉及一种利用移动站或其它等效和相当设备以保密方式对上述电子表格数字签名的方法。在本方法中，待签资料至少包括表格、表格标识符、共享数据，和/或表格所加实质信息，待签资料传递给移动站。待签资料也可以由表格标识符和与表格相关的实质信息生成；例如，在银行传递表格的情况下，可以由银行传递表格的标识符及其实质字段(诸如付费者，收费者和金额字段)中的数据来生成待签资料。

依照本发明，最好在向移动站传递资料之前根据待签资料计算第一散列码。将该散列码与资料连接，以便与资料一起传递，由此允许散列码帮助进行

验证。在资料传递给移动站之后，在移动站对资料签名，然后依照本发明通过对经签字的散列码与签名前由资料计算出的散列码作比较，验证经签名的被传资料的可靠性和一致性。签名还可以通过对实质信息和散列码两者签名来实现，在该情况下，甚至可以保证通过移动站签名的资料对应于传递的供签名资料。

在某些类型的应用中，诸如付费应用中，也可以将传递给移动站的资料传递给第二方，例如银行，由第二方根据接收到的资料计算散列码。可以对在移动站中签名的资料进一步加密，然后将加密后的签名资料从移动站传递给第二方。第二方对加密信息解密，验证签名，根据从移动站接收到的资料计算第二散列码，并将其与根据原始资料计算得到的第一散列码作比较。如果第二方接受数字签名，并且如果第一和第二散列码彼此对应，那么银行将接受通过移动站制作的签名。银行接受签名后，将时间戳盖在经签名的加密资料中，并把资料的签名事务归档。

上述情况是银行客户对从银行接收到的表格进行签名的过程。客户或移动站用户可以与一自动付费机或等效装置进行本地通信。在该情况下，付费机向客户发送付费同意表格。这时，客户与付费机在本地交换消息，然后付费机再发送数字签名数据。但是，付费机可以根据正在进行的通信推断，客户已接受了提供给它的服务和付费表格。付费机可以按所需的付费方式在本地为客户服务，不必等待银行同意。实践中，该情形对应于客户在商店收银机旁用现金卡对产品或服务付费的常规作法，商店为客户提供产品和服务，不需要接触银行以验证付费的可靠性。

还可以在传递给移动站之前对资料加密。在该情况下，必须在签名之前在移动站对资料解密。此作法可以确保只有所需的移动站将接收到待传资料，并保证了信息的安全性。

可以用预先同意的表格叠置、消息结构或任何信息结构生成表格，为表格提供标识符，在向移动站传递表格之前，将预先同意的实质信息填入表格中。散列码可以用例如散列函数来计算。可以用公开和私人密钥方法对消息和/或表格进行签名和/或加密。

在本发明的一个较佳实施例中，在对资料签名之前先将资料和/或其一部分呈现在移动站中。例如，可以呈现收费者、付费者、参考信息和可付金额。还可以要求移动站在向其传递资料之前以签名模式起动。在实践中，这意味着

移动站用户必须输入另一个预定的PIN码，用该PIN码对移动站进行配置，从而按预定签名模式起动。由此，可以使用一种本地认证。

本发明还涉及一种利用移动站按保密方式对电子表格数字签名的系统。该系统最好包括：付费机；与付费机相连、用于生成待签资料并将其传递给移动站的装置，其中所述资料如上定义。在本文中，“付费机”指能够通过电信网与诸如银行、商店等服务提供者通信的任何本地的或在本地操作的自动机。

也可以在计算机中本地实现付费机，该计算机例如通过互联网与服务提供者通信，服务提供者通过互联网提供产品和服务。在该情况下，用本地连接将待签资料从计算机传递到移动站进行签名，或者直接从服务提供者自己的服务器到移动站而不使用本地计算机和本地连接。

依照本发明，付费机包括根据待签资料计算第一散列码的装置。另外，移动站包括用于对传递给它的资料进行签名的签名装置。签名装置可以包括用于存储签名和加密所需算法和密钥的存储器，以及与存储器相连并用于处理资料的处理器，它们实现了签名和有可能的加密。另外，付费机包括通过对移动站中签名得到的散列码与签名前根据资料计算得到的散列码进行比较来验证经签名的被传资料的可靠性。

系统还可以包括一服务器，它与付费机和/或移动站相连，并且由诸如银行或信用卡公司等第二方控制。因此，这种服务器可以由例如银行来维护，并且可以用于实现银行交易。服务器也可以包括用于验证移动站所作数字签名之可靠性的装置，以及用于对服务器与付费机和/或移动机之间传递的资料进行加密和/或解密的加密解密装置。

服务器还可以包括用于对资料盖时间戳的装置，以及在签名认证后将资料之签名事务归档的装置。这些都可以用技术人员已知的方式来实现，因此这里不作详细描述。

与现有技术相比，本发明具有便于实现付费应用、验证事务等优点。由于本发明，移动站可以可靠地用来数字签名，并且可以在许多不同的应用中包括一数字签名。

## 附图说明

以下参照附图，通过几种较佳实施例描述本发明，其中：

图1示出了依照本发明的一个较佳系统；

图 2 示出了依照本发明的另一个较佳系统；

图 3 是一流程图，示出了本发明的一较佳实施例；

图 4 是一示意图，示出了用本发明生成待签字资料的一个较佳例子。

图 1 所示系统包括本地付费机(LPM)2，和与之相连的用于生成待签字资料的装置，其中所述待签字资料包括一种表格、其标识符、共享数据和/或与之相关的实质信息。另外，与之相连的装置 4 将资料传递给移动站。相应地，移动站包括移动站(MS)用来与付费机通信的装置 1。在一实施例中，装置 1 和 4 是用蓝牙技术实现的。关于蓝牙技术的更详细的描述可参见例如 WWW 网页 www.bluetooth.com。还可以使用其它已知的链路访问协议，例如红外接口等。

图 1 所示系统还包括通过 TCP/IP 链路与付费机 2 相连的服务器 8，在本例中，服务器 8 由银行控制。服务器还包括用于验证签名可靠性的装置 9，在实践中，这些装置用于对接收到的加密消息解密并将其包含的数字签名与接收到的用户信息作比较。另外，服务器还包括对签字资料盖时间戳和在签名认证后将签字事务归档的装置 11 和 12。付费机中也可以包括相应的验证装置，在本例中，它们用标号 7 表示。装置 7、11 和 12 还可以具有通过例如 TCP/IP 网络从通用密钥管理服务器取得所需公开密钥的特征。

在图 1 所示的例子中，加密资料包括发票表格和由此计算得到的散列码 H1。在步骤 1，加密资料从付费机 2 传递到移动站 MS。在移动站，所述资料(即发票表格、收费者、付费者、付费金额和编号)被显示在移动电话的显示器(10)上，允许移动站用户检查他/她正在签字的对象。然后，用户利用移动站 MS 对资料和由此计算得到的散列码 H1 签字。在步骤 2，将带有数字签字散列码 $H1_{ds}$ 的资料传递给付费机 2。可以用移动站用户和付费机的公开与私人密钥对付费机 2 和移动站 MS 之间传输的消息加密。在付费机 2 验证了签名的可靠性后，在步骤 3，付费机将结算消息发送给银行。结算是银行活动常用的一种作法，这里不作详细描述。

现在参照图 2，该图所示的系统与图 1 对应，但本例系统的使用方法有些不同。首先，在步骤 1，将付费机生成的资料(例如，表格)传递给银行。然后，在步骤 2，付费机根据资料计算出散列码 H1 并将其传递给移动站签名。该传递可以用本地链路，例如蓝牙连接，来实现。在步骤 3，移动站对接收到的消息进行数字签名，然后将经签字的且可能加密的资料发送给银行。在银行，将根据付费机的资料计算得的散列码与从移动站接收到的、经数字签字的散列码

$H1_{ds}$ 作比较。如果两个散列码匹配，那么同意签字事务。随后，利用服务器加盖时间戳，将如此获得的签字事务归档。银行还可以是诸如信用卡公司等一些其它相应服务的提供者，在该情况下， 除了上述步骤外，还要把对签名可靠性的确认发送给银行、付费机或其它服务提供者。在本例中，在确认签名后，信用卡公司负责交易。

参照图 3，描述本发明的一较佳实施例。首先，在方框 31，生成将由移动站签字的资料。在方框 32，根据所述资料计算第一散列码 H1。接着在方框 45，检查是否必须在传输之前对资料加密。如果必须加密，那么过程进到方框 46，用移动站用户的公开密钥对资料加密。加密后，过程进到方框 33。如果不必对资料加密，那么过程直接进到方框 33，将资料传递给移动站。接着，过程进到方框 34，用户检查移动站显示器上呈现的资料或其中的实质信息，即例如检查发票中收费者和付费金额是否正确。如果在方框 35，付费者同意，那么过程进到方框 37，对资料签字。如果在方框 35，付费者不同意，那么过程进到方框 36，将拒绝消息发送给资料的发送者，例如付费机。然后过程终止。反之，过程从方框 37 进到方框 38。在方框 38，由数字签名和散列码并且可能由接收到的资料生成数据集合体，它包括例如表格中所含的实质信息。此后，在方框 39，将数据集合体传递给付费机，并且过程进到方框 40。在方框 40，将根据所传资料计算得的散列码与经签字的散列码比较。如果散列码匹配，那么在方框 42 接收签名，进一步完成所规定的动作。

如果在方框 40，散列码不匹配，那么重复上述过程。此时，可以用计数器检查资料发送次数是否超过预先允许的次数。即，过程从方框 40 进到方框 43，对计数器的值增 1，即 k＝k+1。然后，过程进到方框 44，检查计数器的值，该值表示资料向移动站发送的次数。如果该值超过预先同意的极限，那么过程进到方框 42，向移动站发送拒绝消息。如果计数器的值小于预先同意的极限，那么过程返回方框 31，重复上述处理过程。

图 4 示出了生成并对表格或资料数字签字的较佳方式。向移动站传递的资料包括表格标识符(方框 51)，所有使用的表格具有专用的标识符。与表格标识符相关的是表格模板(方框 52)；根据这些，应用程序、客户和应用程序的提供者都确切知道各情况下正在使用的表格类型。当生成资料时，如图 4 所示，按顺序链接表格标识符和表格模板。由此计算出第一散列码(方框 54)。

在许多情况下，在将表格传递给移动站签名之前就将表格数据(方框 53)

加至该表格。在本例中，将表格标识符和表格数据按图 4 所示的顺序链接，然后将由此获得的位序列与 16 个随机字节(方框 55)链接。最后将来自方框 54 的第一散列码与这些数据合并。

到此为止，已准备好向移动站传递的资料，由该资料计算出第二散列码(方框 56)。在实践中，第二散列码是在移动站计算的，并将第二散列码加至待签消息(方框 57)。同样，将移动站用户已按需要用个人信息作过补充的用户数据加至待签消息。最好此待签消息还加有来自方框 55 的 16 个随机字节，从而可以验证由传递资料方和移动站用户生成的签字消息的可靠性。在随机字节后面，按顺序设置用户数据和第二散列码。在用户移动站对消息进行数字签名。然后，再将消息传送给第二方，给付费机或者资料源。

总之，进一步重申本发明旨在实现一种方法和系统，其中例示的用户、服务提供者和银行能够验证数字签名的可靠性。其目的是将待签资料与一些用户数据、格式和用户所作的数字签名结合在一起。换句话说，可以将签名与某种链结合。在实践中，所述链对应于目前用户用自己的手签名来确认买卖所使用的链。同样，此方法的目的是按立法者的需要和意图以一种可靠的方法识别签名人。

本发明不限于上述例子，在权利要求书限定的保护范围内可以有许多改变。

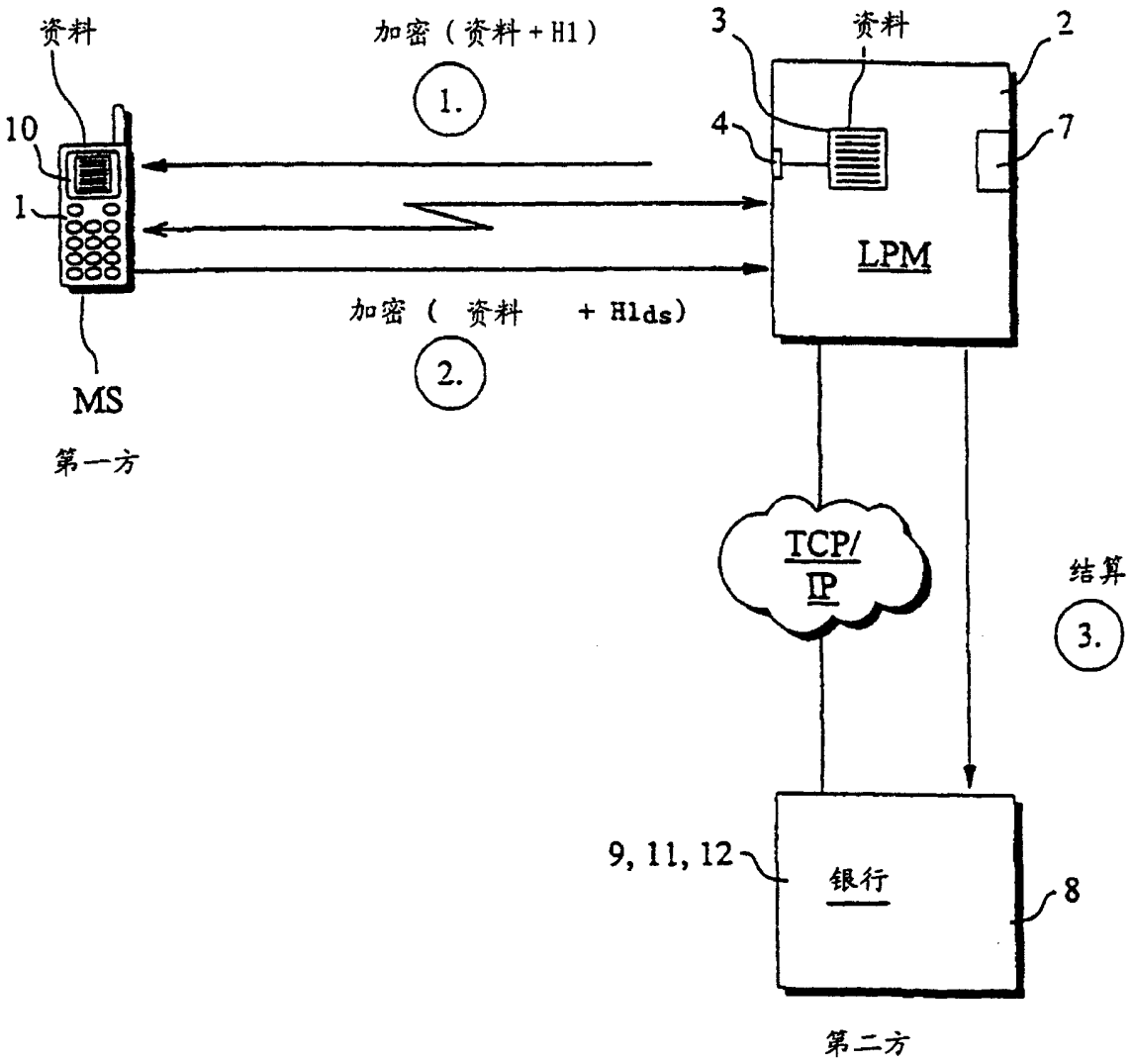

资料
加密（资料+H1）
1.
3
资料
2
10
4
7
1
LPM
加密（ 资料 + H1ds）
2.
MS
第一方
TCP/
IP
结算
3.
9, 11, 12
银行
8
第二方

图 1

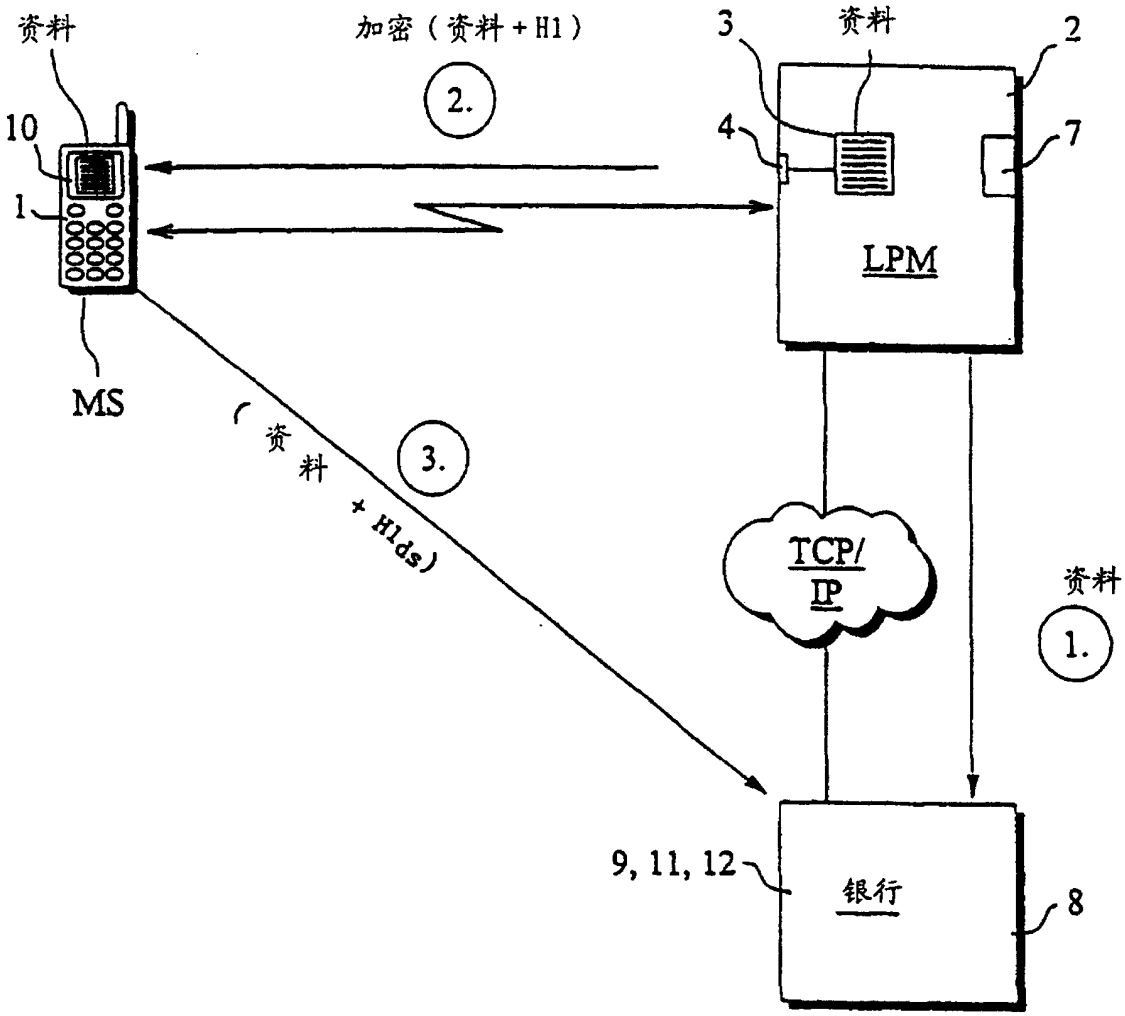



图 2

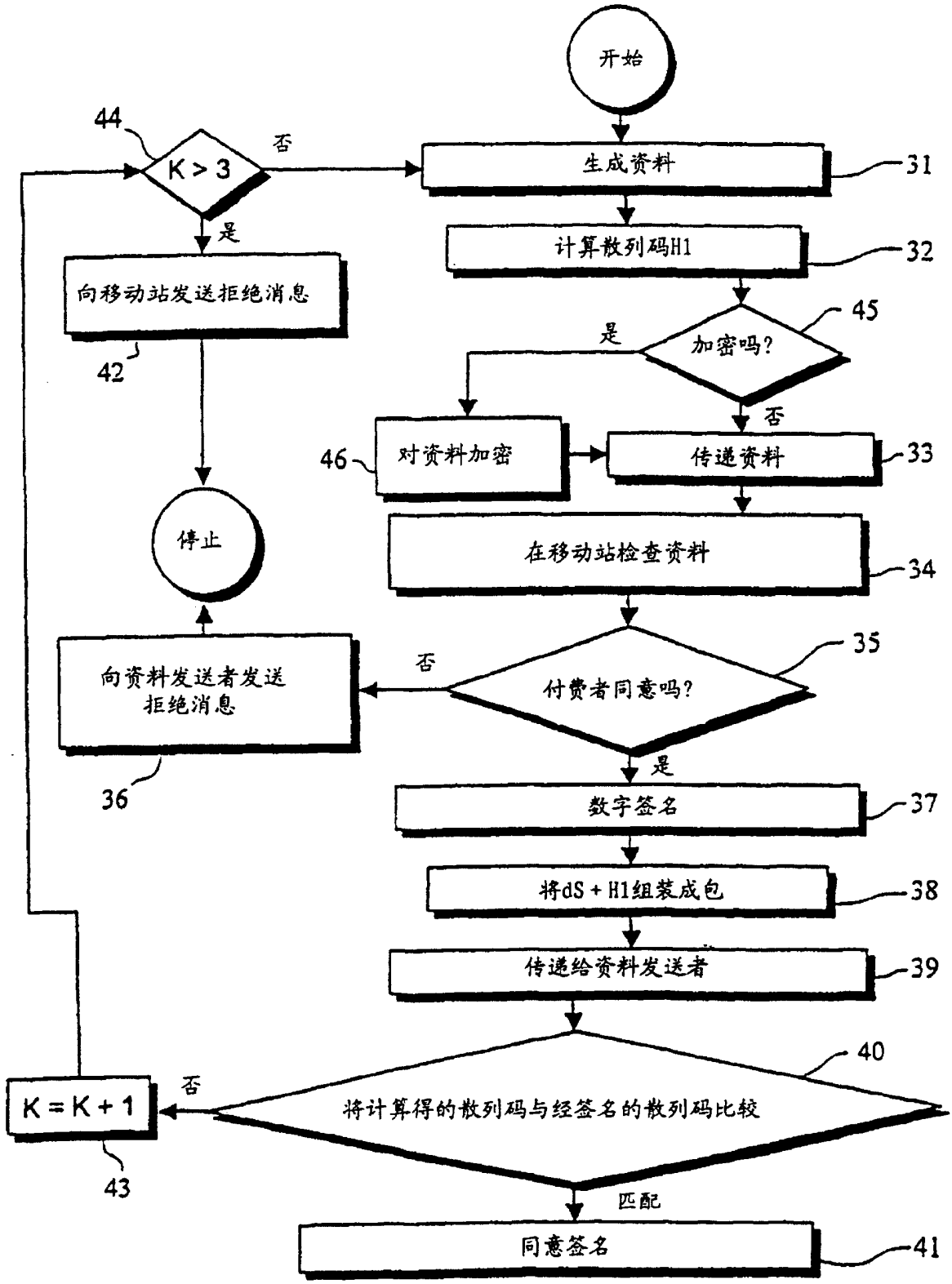

开始
生成资料
31
计算散列码H1
32
加密吗?
45
是
否
对资料加密
46
传递资料
33
在移动站检查资料
34
付费者同意吗?
35
否
是
向资料发送者发送
拒绝消息
36
数字签名
37
将dS + H1组装成包
38
传递给资料发送者
39
将计算得的散列码与经签名的散列码比较
40
否
匹配
K = K + 1
43
同意签名
41
K > 3
44
否
是
向移动站发送拒绝消息
42
停止

图 3

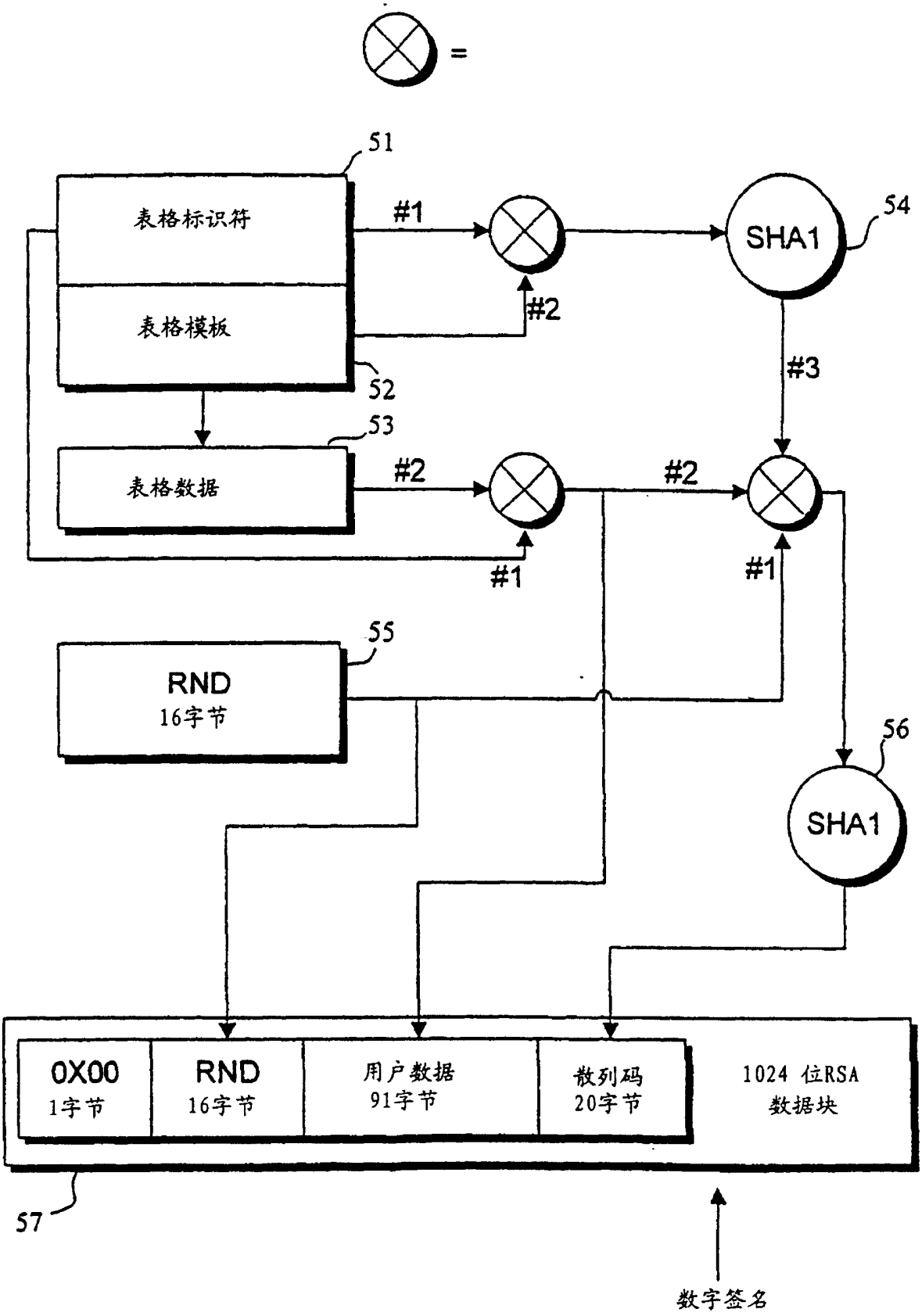

=
51
表格标识符
表格模板
52
#1
#2
SHA1
54
#3
53
表格数据
#2
#2
#1
#1
55
RND
16字节
56
SHA1
0X00
1字节
RND
16字节
用户数据
91字节
散列码
20字节
1024 位RSA
数据块
57
数字签名

图 4