[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04Q 7/22 (2006.01)
H04M 3/42 (2006.01)

[12] 发明专利说明书

专利号 ZL 02808658.9

[45] 授权公告日 2007 年 1 月 24 日

[11] 授权公告号 CN 1297162C

[22] 申请日 2002.3.30 [21] 申请号 02808658.9

[30] 优先权

[32] 2001.4.4 [33] IT [31] TO2001A000321

[86] 国际申请 PCT/EP2002/003590 2002.3.30

[87] 国际公布 WO2002/082838 英 2002.10.17

[85] 进入国家阶段日期 2003.10.22

[73] 专利权人 意大利电信股份公司

地址 意大利米兰

[72] 发明人 马克·斯尼 鲍里斯·摩尔特查诺夫

审查员 张宏伟

[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 李 玲

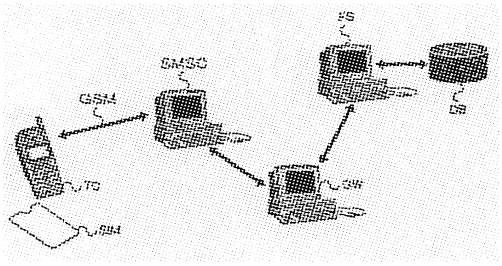
权利要求书 3 页 说明书 6 页 附图 3 页

[54] 发明名称

以受保护的身份传送 SMS 消息的方法

[57] 摘要

本发明涉及一种以受保护的身份传送 SMS 消息的方法，可以防止 SMS 消息的接受方看到主叫方的电话号码以及相应的个人数据，但允许接受方通过发送 SMS 消息来联系主叫方。 在这个过程期间，业务管理员加密包含在消息首部中的用户电话号码，随后再解密以恢复原始的电话号码。



1. 一种以受保护的身份传输 SMS 消息的方法，其中主叫方的电话号码包含在发送的 SMS 消息的首部字段中，用户发送的电话号码可见的 SMS 消息由 SMS 消息业务中心（SMSC）接收和处理，其特征在于，所述 SMS 消息然后转发到转接设备（GW），在此该 SMS 消息用基于适当算法的应用程序以下述方式进行加密，所述加密的电话号码包括利用所述加密算法使用从多个不同的口令中选择的口令加密的主叫方的电话号码的第一部分，以及包含对用于加密所述多个不同口令的口令进行识别的索引的第二部分；然后所述消息传输到目的地，目的地无法从加密的电话号码中追踪到用户的身份，但是可以利用加密的号码应答，因为转接设备（GW）能够解密号码和使号码恢复到原始的形式，然后正确地转发呼叫。

2.如权利要求 1 所述的方法，其特征在于，所述适当的算法是对称可逆的算法，该算法具有用于加密/解密的单个口令，适于作用于连续的号码流来加密不同长度的数据。

3.如权利要求 1 或 2 所述的方法，其特征在于，所述应用程序每次根据管理员应业务提供商的请求分配给布尔变量的值创建由所述索引而索引的口令表，口令可以随机地生成或者对于相同的电话号码口令相同，允许被叫方存储主叫用户所执行的操作历史。

4.如权利要求 1 或 2 所述的方法，其特征在于，所述加密步骤包括如下的步骤:

获得可见的电话号码（1）；

检验电话号码包括多少个字节（2）；

如果号码超过 14 个字节，则不必执行任何操作直接将电话号码发送到输出端（13）；

如果号码没有超过 14 个字节，则将电话号码从用于 SMS 传输的格式转换成十进制数格式（3）；

计算布尔变量的逻辑值（ 4 ）；

如果该布尔变量具有第一逻辑值假，则随机地生成小于口令数目的整数以得到所述表的索引（5）；

如果该布尔变量具有第二逻辑值真，以口令数目作为基数对电话号码进行模运算，得到对相同的电话号码总是相同的索引（6）；

利用所述算法执行加密操作（7）；

检验有多少位十进制数组成该加密号码（8）；

如果十进制数字不超过 14 个十进制数字，则将加密号码从十进制数再次转换成适于 SMS 消息传输的字节矢量（12）；

如果十进制数字超过 14 个十进制数字，则检验加密的号码是否大于或等于 $2*10^{14}$（9）；

如果加密号码小于 $2*10^{14}$，则口令的索引递增口令数目（10）；

如果加密号码大于或等于 $2*10^{14}$，则口令的索引递增口令数目的两倍（11）；

将加密号码从十进制数再次转换成包括两个索引字节的字节矢量（12）；

结束加密操作（13）。

5.如权利要求 4 所述的方法，其特征在于，所述解密步骤包括如下步骤：

获得加密的电话号码（20）；

将电话号码从用于 SMS 传输的格式转换成十进制数格式，提取表示口令表索引的最后两位数（21）；

检验索引值（22）；

如果索引小于口令数目，则得到相应的口令并直接进行解密（27）；

如果索引大于或等于口令数目，则判定索引是否是口令数目的两倍或更多（23）；

如果索引是口令数目的两倍或更多，则加密电话号码加 $2*10^{14}$（25）；

如果索引小于口令数目的两倍，则加密电话号码加 $1*10^{14}$（24）；

则将口令数目用作模基数对索引进行模运算（26）；

进行解密（27）；

将解密的号码再次转换成矢量格式（28）；

结束解密操作（29）。

以受保护的身份传送 SMS 消息的方法

技术领域

本发明涉及电话网数字传输系统，特别是涉及一种以受保护的身份传送 SMS 消息的方法。

背景技术

众所周知，现代电信系统允许传输短 SMS 类型的消息（短消息系统），这种消息可以用电话键盘输入并与声音信号同时显示在电话的显示器上，而不会相互引起干扰。这种字母数字的传输直到最近也是无线网移动电话系统所特有的，但是现在利用连接到固定网的适当装置，例如电话、传真机、电子邮箱（E-mail）等等也能实现这种字母数字的传输。

SMS 消息由不同的字段组成。在这种消息的首部，有包含用户电话号码并被称为 OADC 字段（发起方地址目标代码）的字段，在这种消息的主体，有业务和正文字段。用户电话号码允许系统管理员计费，还允许接受方识别消息的发起方。尽管这个特性是管理员所必需的，但是不能被消息的发送方接受，或者实际上与管理通信隐私的标准相违背，例如当 SMS 消息用于特殊的业务，诸如投票、有奖竞赛等等。最终业务的提供商不准借助于电话号码获得用户的个人数据，但必须能用其它方式到达用户。

目前采用的保护使用音频电话的主叫方身份的方法不适用于这个目的，因为它们通常使电话号码的最后三位数字难以辨认来实现。这样虽然防止了用户被识别，但也使接收呼叫的人无法回话。

从专利文献 WO 00 76231 中可以得知一种在通过移动电话网操作的通信业务中传送消息的方法，该方法允许系统用户之间的匿名通信。每条消息的发送方的电话号码由 SMS 中心用虚拟 ID 替换，而

这种对应关系存入数据库中。接收消息的用户不必知道真正的电话号码就能用虚拟 ID 应答，因为 SMS 中心能够通过查询数据库使这个虚拟 ID 与正确的号码对应起来。这种解决方案暗示了移动网中的结构变化，用于实现数据库和与 SMS 中心的合作。而且数据库的大小不能忽略并随着用户的数目增加。

专利文献 EP 0 899 918 公开了一种用于在一个不同的技术领域，为电子邮件（e-mail）消息生成一个假的源地址的系统。该系统包括假的源地址替换器，它用密钥将真的源地址替换成假的源地址。这从 e-mail 消息中删除了真的源地址，从而使位于真的源地址的发送方匿名。另外，回复邮件的人可以采用对称的加密算法发送恢复的 e-mail。但是，由于 SMS 特殊的结构，这个文件所公开的方法不能传送 SMS 消息。

发明内容

利用以受保护的身份传送 SMS 消息的方法（本发明的主题）可以避免这些难点和解决上述的技术问题，这个过程可以防止 SMS 消息的接受方看到主叫方的电话号码以及相应的个人数据，但允许接受方通过发送 SMS 消息来联系主叫方。

本发明的主题是一种以受保护的身份传送 SMS 消息的方法，其中主叫方的电话号码包含在发送的 SMS 消息的首部字段中，用户发送的电话号码可见的 SMS 消息由 SMS 消息业务中心（SMSC）接收和处理，所述 SMS 消息然后转发到转接设备（GW），在此该 SMS 消息用基于适当算法的应用程序以下述方式进行加密，所述加密的电话号码包括利用所述加密算法使用从多个不同的口令中选择的口令加密的主叫方的电话号码的第一部分，以及包含对用于加密所述多个不同口令的口令进行识别的索引的第二部分；然后所述消息传输到目的地，目的地无法从加密的电话号码中追踪到用户的身份，但是可以利用加密的号码应答，因为转接设备（GW）能够解密号码和使号码恢复到原始的形式，然后正确地转发呼叫。

附图说明

通过下面由非限制性的例子和附图所给出的本发明的优选形式可以使本发明的上述和其它特征变得更清楚，附图中：

图 1 表示 GSM 类型的无线移动系统，其中 SMS 消息根据本发明传送。

图 2 是表示加密操作的流程图；

图 3 是表示解密操作的流程图。

具体实施方式

在以受保护的身份传送 SMS 消息的过程期间，业务管理员加密包含在消息首部中的用户电话号码以免用户的个人数据泄露，随后再解密以恢复原始的电话号码。

图 1 给出了一个 GSM 无线移动系统的例子，其中具有 SIM 卡的 TC 蜂窝电话机发送 SMS 消息，并将它的电话号码显示在 GSM 网上。该消息被叫做 SMSC（短消息业务中心）的 SMS 消息业务中心接收和处理，然后转发到叫做 GW 的转接设备，在此加密主叫方的电话号码。GW 设备，也叫做 SMS 网关，通常将来自 SMSC 的 UDP 消息（用户数据报协议）变换成 IP 消息，然后 IP 消息经 TCP/IP 路由器发送到 TCP/IP（传输控制协议/互联网协议）网。

然后修改后的消息被送到它的目的地，这个目的地可以是具有用户数据库 DB 的 FS 业务提供商，该用户数据库 DB 例如包含用户标识（加密的号码）、用户已经发送的消息数目、发送日期、消息中的信息等等。

如果 FS 业务提供商无法从加密的电话号码中解密用户身份，则仍然可以用加密的号码应答。然后 SMS GW 解密号码以恢复到原始的形式，然后转发该消息。业务提供商显然无法访问 SMS GW，从而看不到电话号码。

用户的电话号码利用包括专门算法的适当的应用程序加密。

选择对称可逆的算法是个好主意，这种算法具有用于加密/解密的单个口令，它作用于连续的号码流来加密不同长度的数据。"流"型算法满足这些要求，这种算法可以字节为单位加密所到达的数据直到末尾。

为了正确使用算法，包括十进制矢量的原始电话号码必须具备下面的特性:

包含国际电码;

不从零开始;

所包含的代码不超过 14 位数。

该应用程序输出最大 16 位数的矢量。这个限制是由于 SMS 消息的 OADC 字段大小所建立的。输出矢量包括不超过所输入电话号码的位数，即 14 的第一加密部分和包括用于加密的口令索引的两位数的第二部分。

创建一个 33 个口令的表，其中每个口令对应一个索引。两位十进制数可以表示的 99 个可能的索引可用于传送更多的信息，正如下面所进一步详细描述的。

加密口令表不包含在源代码中，而是在 SMS GW 模块每次启动加密/解密应用程序时动态地生成。33 个口令不变，但不能从应用程序的源代码或用于计算口令的数学算法中推导出来。所用的算法可以很容易改变。

特别是，该口令可以根据管理员应业务提供商的要求分配给应用程序所考虑的"历史"布尔变量的值从表中随机地选择出来或者可以对相同的电话号码用相同的口令。

如果这个"历史"变量是"真"，则业务提供商可以建立移动用户

所进行的操作过程（story）,并将它存入只有提供商可以访问的装置中。这样，业务提供商可以收集用户的统计数据并存储个人消息的内容，例如用户在有奖竞赛中给出了正确答案。

在解密期间，应用程序输入不超过 16 位十进制数的矢量，该矢量包含加密的电话号码和占据最后两个矢量位置的用来加密的口令索引。

该"真""历史"变量不必解密，因为它可以从口令索引所属的数值范围中推导出来。

输出中，应用程序恢复不超过 14 位十进制数的原始电话号码，在国际电码的开始没有零。

加密用户电话号码的各个操作的更多细节在图 2 所示的流程图中给出。

在开始阶段 1，即获得消息首部 OADC 字段中的电话号码之后，检验它由多少个字节组成，阶段 2 。如果长度不超过 14 个字节，则不必执行任何操作直接发送到输出端，阶段 13。否则，电话号码从用于 SMS 传输的格式转换成十进制数格式，阶段 3。SMS 格式实际上包括 14 个字节的矢量，每个字节表示电话号码从 0 到 9 的数字，它必须转换成十进制，以便可以进行随后的操作。

下一个阶段 4 检验"历史"布尔变量是否已经设置成"真"。如果情况不是这样，即逻辑值是"假"，则用叫做 RAND（32）的函数随机生成一个小于 33 的整数以获得口令表索引。否则，用 MOD_{33}（OADC）函数对电话号码进行基数为 33 的模运算，以给出索引，相同的数字索引总是相同，阶段 6。现在众所周知基数为 33 的模运算就是将号码除以 33，直到余数小于 33。余数就是口令表索引。

在下一阶段 7，如果以上述两种方式之一计算的电话号码和口令表索引可以获得，则可以利用选定的"流"对称算法进行加密。

阶段 8 检验有多少个十进制数字组成加密号码。如果它包括不超过 14 位的十进制数字，则从十进位数再次转换成适于 SMS 消息传输的字节矢量，两个索引字节添加到末尾，阶段 12，以便在操作结

束时恢复，阶段 13。但是，如果它包括 14 位以上的十进制数字，则检验它比 $2*10^{14}$ 多还是少，阶段 9。如果小于 $2*10^{14}$，则索引加 33，阶段 10，而如果大于或等于 $2*10^{14}$，则索引加 66，阶段 11。

这样，口令表索引可以是在 0-32、33-65、66-99 的三个范围之一，因此提供这样的信息，即加密号码除了 14 位十进制数字以外还包括可以分别是 0、1 或 2 的第 15 位数字。显然，不同于 00、33 或 66 的索引总是确定相同的口令。

与上一种情况相同，十进制数再次转换成包括两个索引字节的字节矢量，如此获得 16 字节的矢量，阶段 12，然后输出，阶段 13。

解密用户电话号码的各个操作的更多细节在图 3 所示的流程图中给出。

在初始化的第一阶段，阶段 20，即获得消息 OADC 字段中的加密电话号码之后，它通过提取表示口令表索引的最后两位数字从用于 SMS 传输的矢量格式转换成十进制数，阶段 21。

然后阶段 22 检验索引值。如果索引小于 33，则可以找到相应的口令并直接进行解密，阶段 27。获得的号码再次转换成适于 SMS 消息传输的矢量，阶段 28，然后输出，阶段 29。

但是，如果索引大于或等于 33，检验它是否大于或等于 66，阶段 23。如果是，则密码电话号码加 $2*10^{14}$，阶段 25，否则加 $1*10^{14}$，阶段 24，如此获得原始的加密号码。在这两种情况下，索引进行基数为 33 的模运算，阶段 26，以获得在范围 0-32 的值，然后解密，阶段 27，再次转换成矢量格式，阶段 28，然后结束，阶段 29。

显然，用非限制性的例子给出了这个说明书。可以进行变型和改进，但没有超出权利要求书的保护范围。

图1

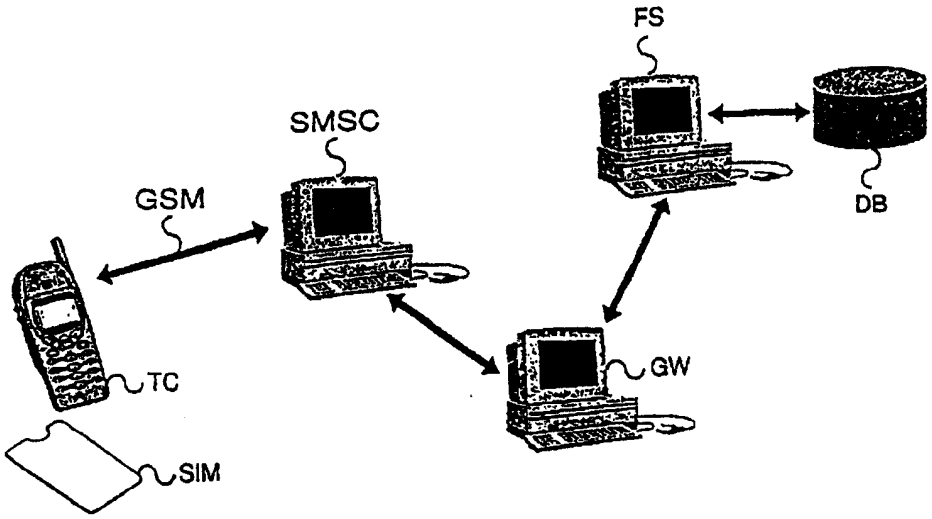


图2

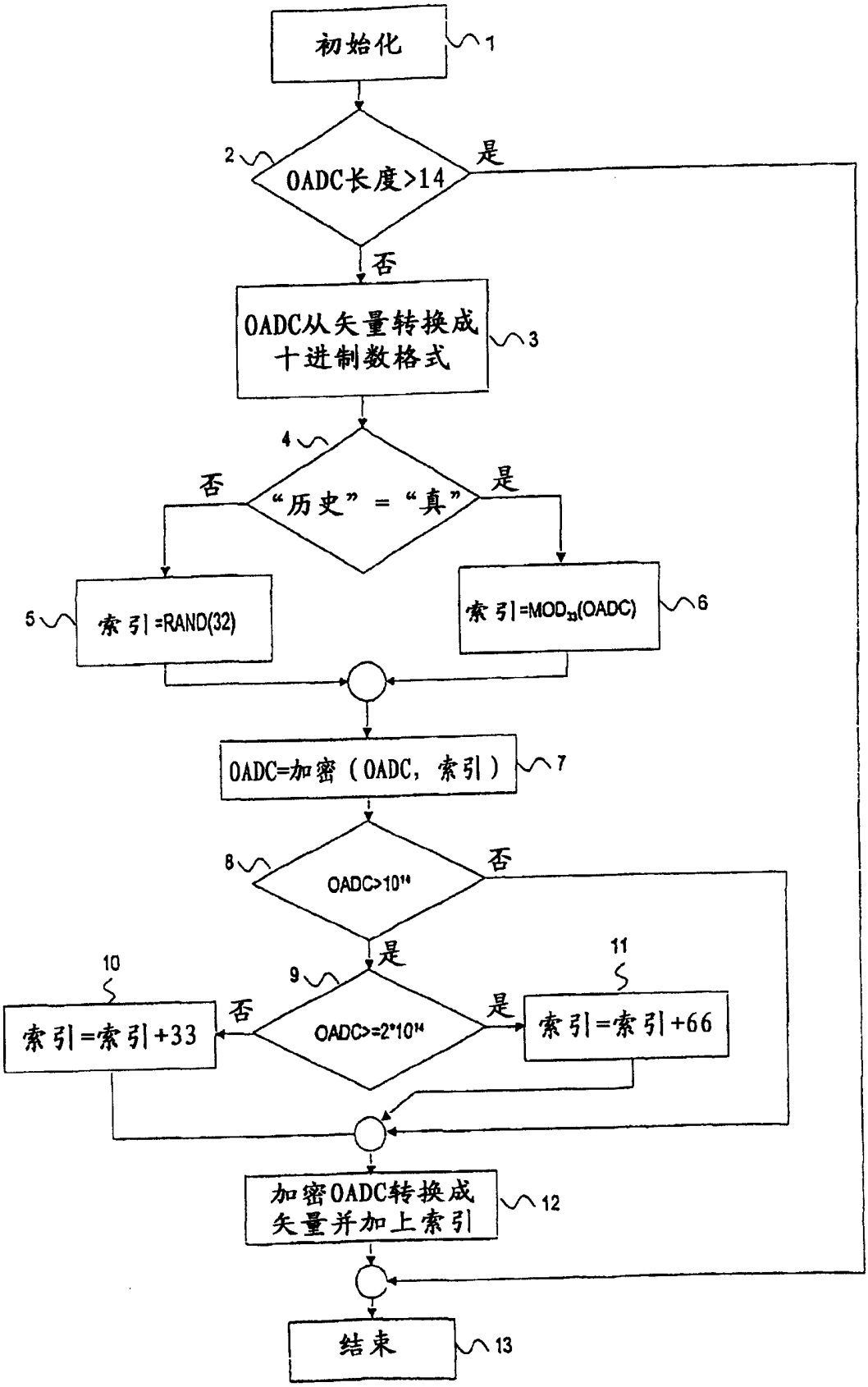
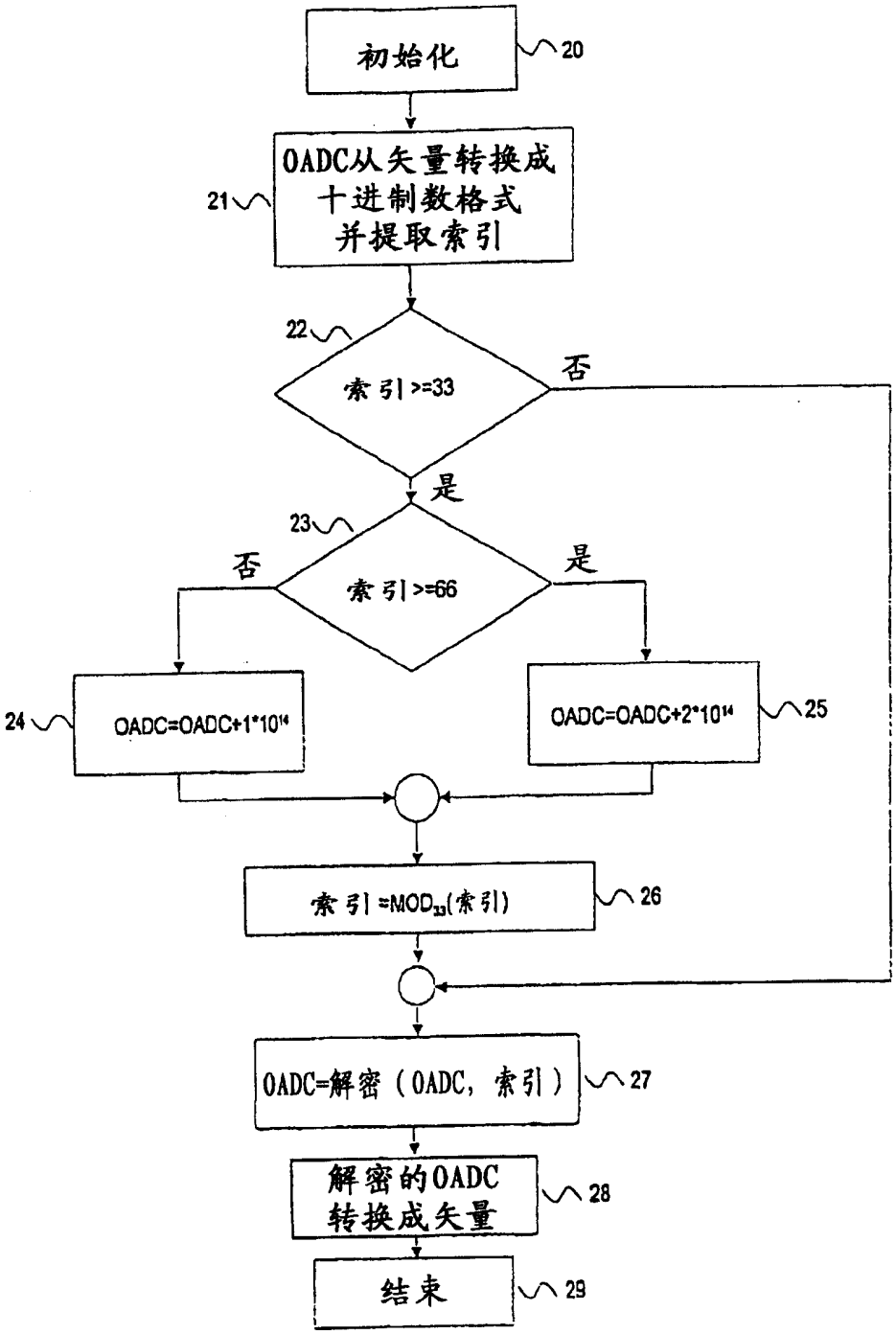

初始化
1
2
OADC长度>14
是
否
OADC从矢量转换成
十进制数格式
3
4
“历史”=“真”
否
是
5
索引=RAND(32)
索引=MOD33(OADC)
6
OADC=加密（OADC，索引）
7
8
OADC>10^14
否
是
10
9
OADC>=2*10^14
否
是
11
索引=索引+33
索引=索引+66
加密OADC转换成
矢量并加上索引
12
结束
13

图3


初始化
20
OADC从矢量转换成十进制数格式并提取索引
21
22
索引>=33
否
是
23
索引>=66
否
是
24
OADC=OADC+1*10^14
OADC=OADC+2*10^14
25
索引=MOD33(索引)
26
OADC=解密（OADC，索引）
27
解密的OADC转换成矢量
28
结束
29