[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06K 17/00

[12] 发明专利说明书

[21] ZL 专利号 97104327.2

[45] 授权公告日 2004 年 1 月 7 日

[11] 授权公告号 CN 1133954C

[22] 申请日 1997.5.21 [21] 申请号 97104327.2

[30] 优先权

[32] 1996. 5.22 [33] JP [31] 126184/1996

[71] 专利权人 日本电气株式会社

地址 日本国东京都

[72] 发明人 松本真理子

审查员 高一昂

[74] 专利代理机构 中科专利商标代理有限责任公司

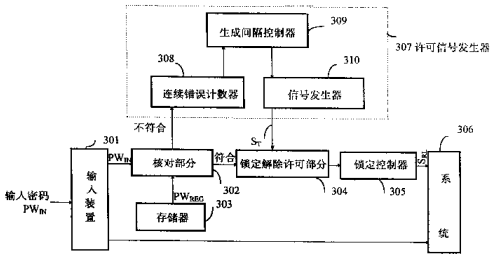
代理人 刘晓峰 朱进桂

权利要求书 2 页 说明书 12 页 附图 11 页

[54] 发明名称 保密信息识别系统

[57] 摘要

在一个保密信息识别系统中，输入密码被与已注册的密码进行比较并再次产生一个许可信号。当比较结果表示相符时给出一锁定解除许可。另外，输入密码被与已注册的密码进行比较，当比较表示相符时每次给出一个锁定解除许可并产生一个许可信号。当在比较结果中的不符合事件的数目增多时，许可信号的生成周期被延长。其结果，密码不容易被破译，并且即使在输入一个错误密码后密码输入功能也不会被锁定。



ISSN1008-4274

1.根据输入信息是否与预定信息相符提供认可的识别系统，包括：

用于将输入信息与预先设定的信息进行比较以产生一表示符合或不符合的比较结果的一信息检验器；其特征在于还包含：

用于产生一基准时钟信号的一基准振荡器；

用于从基准时钟信号产生多个时钟信号的一分频器，时钟信号具有不同的频率；

用于计算表示不符合的比较结果并产生一不符合计数的一计数器；

用于从建立在不符合计数基础之上的作为许可信号的时钟信号中选择出一个信号的一选择器；及

根据许可信号和比较结果来提供认可的一控制器。

2.根据权利要求 1 所述的识别系统，其特征在于：

信息检验器产生与从选择器接收到的许可信号相对应的比较结果及

当从信息检验器接收到表示符合的比较结果时，控制器提供认可。

3.根据权利要求 1 所述的识别系统，其特征在于当从定时发生器接收到许可信息而同时比较结果表示符合时，控制器提供认可。

4.根据权利要求 1 所述的系统，其特征在于其中当不符合的计数增加时，选择器选择一个具有较低频率的时钟信号。

5.根据权利要求 1 所述的系统，其特征在于选择器根据基于不符合计数产生的随机数选择其中一个时钟信号。

6.根据权利要求 2 或 3 所述的系统，其特征在于选择器将基于输入信息的比较结果的许可信号生成间隔延长。

7.根据权利要求 2 或 3 所述的识别系统，其特征在于选择器根据由输入信息的比较结果所产生的随机数选择时钟信号中的一个。

8.根据权利要求 6 所述的系统，其特征在于选择器随表示不符合增加的比较结果数目延长许可信号的生成间隔。

9.一种根据输入信息是否与预定信息相符来提供认可的方法，包含如下步骤：

将输入信息与预先设定的信息进行比较，并产生表示符合或不符合的比较结果；其特征在于还包含如下的步骤：

产生一个基准时钟信号；

由基准时钟信号产生多个时钟信号，时钟信号具有不同的频率；

计数表示不相符合的比较结果以产生不符合的计数；

根据不符合的计数从作为许可信号的时钟信号中选择一个以产生许可信号；及

根据许可信号和比较结果来提供认可。

保密信息识别系统

技术领域

本发明涉及个人信息识别系统，特别是涉及用于检验输入保密信息的识别系统。

背景技术

在自动出纳机及类似的装备在银行系统中的仪器中，使用者通过其输入的保密信息诸如密码而被验证，从而防止了其它人使用其帐户。亦即在此种系统中，输入的密码被与预先设定的密码进行比较，从而当两个密码彼此相吻合时该机器被允许开始操作。在这样的一种系统中，预先设定的密码通常为一固定的密码。众所周知的有几类这样的系统，其中第一类允许使用者无限次地输入密码，而对于另一类系统如果输入的密码次数超过某一给定的数目时则密码输入功能被锁定例如会失灵。（参考日本未审查专利公开 No.62-219048）。

如上描述的传统的系统具有如下的缺点。在第一类系统中，由于其允许使用者无数次地输入密码，从而密码容易被例如使用计算机而破译，在其它类的系统中，如果密码的输入次数大于某一给定数值，则密码输入功能被锁定从而无法继续输入密码，当意外地输入错误密码时，密码输入功能被锁定，在这种情况下即使是真正的使用者也无法使用机器。

发明内容

本发明已被用来解决本领域中的以上问题，因此本发明的一个目的是提供一种保密信息很难破译且信息输入功能不被锁定的系统。

根据本发明，根据输入信息是否与预定信息相符提供认可的识别系统，包括：用于将输入信息与预先设定的信息进行比较以产生一表示符合或不符合的比较结果的一信息检验器；其还包含：用于产生一基准时

钟信号的一基准振荡器；用于从基准时钟信号产生多个时钟信号的一分频器，时钟信号具有不同的频率；用于计算表示不符合的比较结果并产生一不符合计数的一计数器；用于从建立在不符合计数基础之上的作为许可信号的时钟信号中选择出一个信号的一选择器；及根据许可信号和比较结果来提供认可的一控制器。

一种通过核对所输入的信息是否与预先设定的信息一致而进行验证的系统其包括一第一控制器，其根据输入信息的核对结果而来改变许可定时，还包含一第二控制器，当在许可定时期间核对结果表明相一致时其进行验证。根据输入信息的核对结果第一控制器可延长许可定时的时限。最好地，当表示非吻合的核对结果的次数增加时，第一控制器可延长许可定时的时限。另外，第一控制器可根据输入信息的核对结果随机地改变许可定时的时限。

根据本发明的一个方面，输入信息与预先设定的信息每比较一次则产生许可信号，当比较结果表明相吻合时，则批准进行锁定解除。产生许可信号的周期或间隔根据比较结果中的非吻合事件的数目而变化。

根据本发明的另一个方面，输入信息与预先设定的信息进行比较，当比较结果表示相吻合时则根据产生的许可信号而给予批准。产生许可信号的间隔或周期根据比较结果中非吻合事件的数目而变化。

因此，即使输入所有可能的保密信息，也不会产生吻合。这样的好处在于即使使用计算机或类似工具也不容易破译保密信息。另外，根据本发明，保密信息输入功能不会被锁定。这样又具有另外一个好处，即使在输入不正确信息后，通过输入预先设定的信息仍可解除系统的锁定。

附图说明

通过如下的详细描述并结合相应的附图会使本发明的以上及其它的目的及优点变得更清楚，其中：

图 1 为根据本发明的实施例的密码识别系统的结构方框图；

图 2 为对图 1 的密码识别系统的操作流程图；

图 3 为图 1 中密码识别系统的操作实例的时序图；

图 4 为图 1 中密码识别系统的另一个操作实例的时序图；

图 5 为为根据本发明的另一个实施例的密码识别系统的结构方框图；

图 6 为图 5 的密码信息识别系统的操作流程图；

图 7 为图 5 的密码信息识别系统的操作实例的时序图；

图 8 为图 5 的密码识别系统的另一个操作实例的时序图；

图 9 为显示图 1 或图 5 的许可信号发生器的第一实例的详细方框图；

图 1 0 为图 9 的许可信号发生器的操作时序图；及

图 1 1 为图 1 或图 5 的许可信号发生器的第二实例的详细方框图。

具体实施方式

参考图 1，根据本发明一个实施例的密码识别系统具有如下的结构。使用者使用键板等输入装置 1 0 1 输入密码 PW_{IN} 和其它需要的信息。核对许可部分 1 0 2 将输入密码 PW_{IN} 转换为与许可信号 S_T 相对应的核对部分 1 0 3 。换句话说，核对许可部分 1 0 2 具有根据许可信号 S_T 而许可一核对操作的功能。核对部分 1 0 3 通过将输入密码 PW_{IN} 与一预先存储在存储器 104 中的已注册的密码 PW_{REG} 进行比较来对输入密码 PW_{IN} 进行核对。当比较的结果为“符合”时，锁定控制器 1 0 5 将系统 1 0 6 的锁定解除。许可信号发生器 1 0 7 从核对部分 1 0 3 接收比较结果并根据比较结果来改变产生的许可信号 S_T 的周期并产生许可信号 S_T 。

许可信号发生器 1 0 7 包含一连续错误计数器 1 0 8，其用于计算从核对部分 1 0 3 接收到的“不符合”连续比较结果的数目。如后面将要描述的，生成间隔控制器 1 0 9 根据计数器 1 0 8 的计数来控制许可信号 S_T 的生成间隔（或周期）。信号发生器 1 1 0 在控制器 1 0 9 的控制下产生许可信号 S_T 并将其提供到核对许可部分 1 0 2 。

参考图 2，许可信号发生器 1 0 7 产生作为触发信号的许可信号 S_T 用于允许核对操作。通常地，许可信号发生器 1 0 7 在最小的间隔产生许可信号 S_T 。当密码 PW_{IN} 通过输入装置 101(步骤 S201)被输入时，

核对许可部分 102等待一个由许可信号发生器107（步骤S202）产生的许可信号。当检测到一个许可信号 S_T 时（步骤S202为是），核对部分103将输入密码 PW_{IN} 与事先已存在存储器 104 中的已注册的密码 PW_{REG} 进行比较(步骤 S203)。如果比较的结果为“符合”，许可信号 S_T 的生成间隔被减至最小（步骤S204），然后锁定控制器105操作解除系统106的锁定（步骤S205），从而允许系统106工作（步骤S206）。

另一方面，如果输入密码 PW_{IN} 与已注册的密码 PW_{REG} 不同,核对部分 103 检测到不符合(步骤 S203)。许可信号发生器107的连续错误计数器108计数输入密码中的连续错误，而生成间隔控制器109根据计数器 108 的计数来设定一个许可信号生成间隔（步骤S207）。在此实施例中，当计数增大时许可信号生成间隔（周期）被延长。信号发生器110在这样所设定的周期或间隔产生许可信号 S_T 。

在这样的许可信号生成间隔（周期）已被延长的状态下，即使密码 PW_{IN2} 在一短暂时间的间隔后又重新被输入,由于在延长的许可信号生成间隔没有产生许可信号,核对许可部分 102 不允许核对部分 103 的核对操作。而使用者未得到任何许可信号生成信息。当他又输入一个密码 PW_{IN3} 则在许可信号生成间隔的一段间隔后产生许可信号 S_T ,核对许可部分 102 允许在核对部分 103 内的核对操作(步骤 S202 为是)。相应地，核对部分103将输入密码 PW_{IN3} 与注册的密码 PW_{REG} 进行比较(步骤 S203)。本系统的一个重要特征是输入密码 PW_{IN2} 不受核对的支配。也就是说,即使输入密码 PW_{IN2} 为一已注册的密码,仍不允许系统 106 工作。

如果通过输入密码 PW_{IN3} 又被检测到不符合,则连续错误的计数增加 1。其结果，生成间隔控制器109进一步延长许可信号生成间隔（步骤 S207），这意味着核对部分103的不工作时间也相应地延长了。如果通过输入密码 PW_{IN3} 而检测到符合，许可信号生成间隔被设定在最小值（步骤S204），锁定被解除（步骤S205），同时系统106被允许工作（步骤S206）。

对如下的一种情况须引起注意，即在输入N次的错误密码后输入一

次已注册的密码。在这种情况下，在与连续错误的数目N相对应的许可信号生成间隔产生许可信号 S_T 。当输入一个注册的密码 PW_{REG} 并且核对许可部分 102 接收到一个许可信号 S_T ，该许可信号 S_T 是在与连续错误的数目N相对应的许可信号生成间隔的一段间隔之后产生的，核对许可部分１０２将输入密码 PW_{IN} 输出到核对部分 103 来许可核对操作。当核对部分１０３将输入密码 PW_{IN} 与已注册的密码 PW_{REG} 进行比较并检测到符合时,许可信号生成间隔返回到最小值(步骤 S204),锁定被解除(步骤S205),从而系统 106 被允许工作(步骤S206)。

下面将参考图 3 和图 4 的时序图来对许可信号生成间隔进行描述。图 3 和图 4 都示出了输入密码 PW_{IN} ，许可信号 S_T ，和用于表示核对部分１０３的比较结果（符合或不符合）的比较输出以及从锁定控制器１０５输出的锁定解除信号 S_{RL} 。图 3 和图 4 的每张图中，水平轴代表时间而比较输出的固定部分和锁定解除信号 S_{RL} 代表有效状态而其余的部分代表待用状态。

在图 3 （b）的许可信号 S_T 中，用高电平表示许可。图 4 （b）的许可信号 S_T 被用作触发脉冲并在触发脉冲的上升沿完成操作。当没有密码输入时则即使产生许可信号 S_T 也不进行检对操作，在此实例中，为了简化描述，假设已注册的密码 PW_{REG} 为"6"则仅接受从“０”到“９”的输入密码 PW_{IN} 。

参照图 3，在正常状态下，许可信号生成间隔被设定在最小值（在此例中为“０”），则一旦输入已注册的密码 PW_{REG} “６”，锁定就被解除同时系统１０６被允许工作。

对这样的一种情况应引起注意，即当目的在于要破译密码的使用者输入“０”到“９”的任意可试的密码的情况。当输入第一个密码 PW_{IN} “０”时，核对部分１０３检测到不符合则连续错误的数字为１。其结果，原始状态为“０”的许可信号生成间隔变为“１”。当输入另一个密码 PW_{IN2} "1"时,由于没有产生许可信号 S_T 则不进行核对操作。由于使用者不知道许可信号生成信息，他输入了另一个密码 PW_{IN3} "2"。由于此后生成了许可信号 S_T ，则输入信号被与已注册的密码 PW_{REG} 进行比较。其结果，又检测到一次不符合，从而连续错误的数目变为 2 同

时许可信号生成间隔也变为“2”。

当相继输入下一个密码 PW_{IN4} 和 PW_{IN5} (例如“3”和“4”) 时，由于没有产生许可信号从而不进行核对操作。当再次输入另一个密码 PW_{IN6} "5"时,之后产生一个许可信号 S_T 从而输入密码 PW_{IN6} 受核对操作的控制。由于检测到不符合，连续错误的数目变为3且许可信号生成间隔变为“3”。

虽然此后输入一已注册的密码 PW_{IN7} “6”，由于没有产生许可信号 S_T 从而核对部分103不进行其核对操作。接着，相继输入密码 PW_{IN8} “7”到 PW_{IN10} “9”。由于在输入密码 PW_{IN10} “9”后产生了一许可信号 S_T ，仅该密码受核对操作的控制。由于又检测到一次不符合，连续错误的数目变为4且许可信号生成间隔也变为“4”。此后，当没有密码输入时核对部分103不再工作。因此，符合或不符合均未被检测到，许可信号生成间隔保持在“4”。

即使当此后输入已注册的密码 PW_{IN11} “6”时，直到产生许可信号 S_T 才进行核对操作。当在许可信号生成间隔“4”的一段间隔之后的时间 T_1 产生许可信号 S_T 时，核对部分103执行其核对操作。由于在该时间检测到了密码符合，锁定被解除而系统106被允许工作。

参考图4，针对图3中的实例，在通常的状态下，许可信号生成间隔被设定到最小值。在此例中，许可信号 S_T 被作为连续上升的触发信号而产生。如果在此状态下输入已注册的密码 PW_{REG} “6”，锁定立即被解除而系统106被允许工作。

在使用者旨在想破译密码的情况下，输入从“0”到“9“的全部可试的密码，正如图3的实例中的情况，随比较结果中的不符合连续事件的数目上升，许可信号生成间隔被延长。在连续错误的数目变为4和许可信号生成间隔变为“4”后，在没有输入密码时核对部分103不工作。因此，没有检测到符合或不符合且许可信号生成间隔维持在“4”。

即使当此后输入一已注册的密码 PW_{IN11} “6”，则直到产生许可信号 S_T 才会进行核对操作。当在许可信号生成间隔“4”的间隔后的时间 T_1 产生许可信号 S_T 时，核对部分103执行其核对操作。由于在该时间检测到密码符合，锁定被解除且系统106被允许工作。

参考图5，根据本发明的另一个实施例的密码识别系统具有如下的结构。使用者使用键板等输入装置301输入密码 PW_{IN} 和其它必要的信息。密码 PW_{IN} 被输出到核对部分 302, 核对部分 302 通过将输入密码与事先已存储在存储器 303 中的已注册的密码 PW_{REG} 进行比较来核对输入密码 PW_{IN} 。核对部分302的比较结果被输出到锁定解除许可部分304和许可信号发生器307。锁定解除许可部分304根据“符合”的比较结果和许可信号 S_T 将锁定解除许可信号输出到锁定控制器305。换句话说，锁定解除许可部分304具有根据比较结果和许可信号 S_T 许可锁定解除的功能。当从锁定解除许可部分304接收到锁定解除许可信号时，锁定控制器305将系统306的锁定解除。许可信号发生器307从核对部分302接收到比较结果并通过改变基于比较结果的许可信号 S_T 的生成周期来产生许可信号 S_T 。

许可信号发生器307包括一连续错误计数器308，其用于计算从核对部分302接收到的“不符合”连续比较结果的数目。如后面将要描述的，生成间隔控制器309根据计数器308的计数来控制许可信号 S_T 的生成间隔（周期）。信号发生器310在控制器309的控制下产生许可信号 S_T 并将其提供到锁定解除许可部分304。

参考图6，许可信号发生器307产生作为触发信号的许可信号 S_T 用于许可锁定解除操作。通常地，许可信号发生器307在最小的间隔产生许可信号 S_T 。当通过输入装置301输入密码 PW_{IN} 时(步骤S401), 核对部分 302 将输入密码 PW_{IN} 与事先存储在存储器 303 中的已注册的密码 PW_{REG} 进行比较(步骤 S402)。如果比较结果是“符合”，锁定解除许可部分304等待由许可信号发生器307产生的许可信号 S_T（步骤S403）。当接收到一个许可信号 S_T 时（步骤S403为是），在许可信号生成间隔被重新设定到最小值后（步骤S404），锁定解除许可部分304将锁定解除许可信号输出到锁定控制器305。根据锁定解除许可信号，锁定控制器305工作以解除系统306的锁定（步骤S405），从而允许其工作（步骤 S406）。

另一方面，如果输入密码 PW_{IN} 已注册的密码 PW_{REG} 不同，核对部分302检测到不符合（步骤S402）。许可信号发生器307

的连续错误计数器３０８计算输入密码中的错误，生成间隔控制器３０９根据计数器 ３０８的计数来设定一许可信号生成间隔。信号发生器３１０产生许可信号 S_T ，其生成间隔（周期）根据所设定的许可信号生成间隔而被延长（步骤Ｓ４０７）。

如果在这种状态下输入密码 PW_{IN2} ，并检测到不符合，错误计数增加１而因此许可信号生成间隔再被延长。另一方面，即使在这种状态下检测到符合，锁定解除许可部分３０４不立即许可锁定解除，其原因是由于被延长的许可信号生成间隔内无许可信号产生。

使用者不知道任何许可信号生成信息。当他又输入一个密码 PW_{IN3} 时，则执行核对操作，在许可信号生成间隔的间隔之后产生一许可信号。如果密码 PW_{IN3} 的比较结果为“不符合”，控制返回到密码输入等待状态（步骤 Ｓ４０１）。如果比较结果是“符合”，许可信号生成间隔被调为最小值（步骤Ｓ４０４），锁定被解除（步骤Ｓ４０５），系统３０６被允许工作。如上所述的情况下，本系统的一个重要特征是即使输入密码是已注册的密码且比较结果是“符合”时，锁定也不会被解除。如果通过输入密码 PW_{IN3} 又检测到一次不符合,错误计数增加１。其结果是，许可信号生成间隔再次被延长，其意味着防止锁定解除时间也相应地被延长。

一个值得注意的情况是，当在输入Ｎ次错误密码后输入一次已注册的密码。在这种情况下，在与错误数目Ｎ相对应的许可信号生成间隔产生许可信号 S_T 。当输入一个已注册的密码 PW_{REG} 时，核对部分３０２检测到符合而锁定解除许可部分３０４检测到一许可信号 S_T ，该信号是在与错误的数目Ｎ对应的许可信号生成间隔的间隔之后产生的，同时锁定解除许可部分３０４批准锁定解除操作。然后，许可信号生成间隔返回到最小值（步骤Ｓ４０４），锁定被解除（步骤Ｓ４０５），而系统３０６被允许工作（步骤Ｓ４０６）。

下面，将参考图７和图８的时序图来对许可信号生成间隔进行描述。图７和图８都示出了输入密码 PW_{IN} 、许可信号 S_T 、用于表示核对部分３０２的比较结果的比较输出及从锁定控制器３０５输出的锁定解除信号 S_{RL} 。在图７和图８中，水平轴代表时间而核对输出的固定

部分和锁定解除信号 S_{RL} 代表有效状态而虚线代表待用状态。

在图7（b）的许可信号 S_T 中，用一高电平代表许可。图8（b）的许可信号 S_T 被作为触发脉冲并在触发脉冲的上升沿完成操作。在无密码输入时不进行核对操作。在此实例中，为了简化描述，假设已注册的密码 PW_{REG} 为“6”而仅接受从“0”到“9”的输入密码 PW_{IN} 。

参考图7，在通常状态下，许可信号生成间隔被设定到最小值（此例中为“0”），只要一旦输入已注册的密码 PW_{REG} “6”锁定即被解除而系统306被允许工作。

对这样的一种情况应引起注意，即当使用者旨在通过输入从“0”到“9”的全部可试用的密码来破译密码。当输入第一个密码“0”，核对部分302检测到不符合而错误的数目变为1。其结果，在原始状态为“0”的许可信号生成间隔变为“1”。当输入另一个密码“1”时，核对部分 302检测到不符合而因此错误的数目变为2且许可信号生成间隔为“2”。然后，从“3”到“5”的密码 PW_{IN} 被依次输入，从而错误的数目变为6而许可信号生成间隔变为“6”。

当随后输入一已注册的密码 PW_{IN} “6”时，核对部分302检测到符合。然而，由于没有产生许可信号 S_T ，从而锁定解除许可部分304不允许锁定解除。接着，相继输入从“7”到“9”的密码 PW_{IN} ，从而错误的数目变为9且许可信号生成间隔变为"9"。此后，当不进行密码输入时核对部分302不再工作。因此，检测不到符合或不符合信息而许可信号生成间隔维持在“9”。

当此后输入一已注册的密码 PW_{IN} "6"时，检测到符合但要直到产生许可信号 S_T 锁定才会被解除.当在许可信号生成间隔"9"的间隔之后的时间 T_2 产生许可信号 S_T 时,许可信号生成间隔被调到最小值,锁定被解除，而系统 306被允许工作。

参考图8，正如图7中的例子一样，在通常状态下，许可信号生成间隔为最小而许可信号 S_T 在最小间隔连续上升。如果在此状态下输入已注册的密码 PW_{REG} “6”，锁定立即被解除且系统306被允许工作。

对这样的一种情况需引起注意即当使用者输入从“0”到“9”间

的全部可试用的密码旨在破译密码的情况。在这种情况下，正如图7中例子的情况一样，当在比较结果中的不符合事件的数目增加时，许可信号生成间隔被延长。在错误的数目变为“9”及许可信号生成间隔变为“9”后，由于没有密码输入从而核对部分302不工作。由于既未检测到符合也未检测到不符合，从而许可信号生成间隔被维持在“9”。

当此后输入已注册的密码 PW_{REG} “6”时，检测到符合，但由于未产生许可信号 S_T 从而不能解除锁定。当在许可信号生成间隔“9”的间隔之后的时间 T_2 产生许可信号 S_T 时，许可信号生成间隔被调到最小值，锁定被解除，系统306被允许工作。

参考图9，许可信号发生器107或307可由如下的部件组成。例如，基准振荡器501向计数器502输出一基准时钟信号CLK。计数器502针对基准时钟信号CLK的时钟脉冲执行一计数操作。逻辑电路503接收计数器502的输出并产生基于计数器502的计数输出的不同周期的时钟信号 S_{T0} 到 S_{T2} 。计数器505从核对部分103或302接收不符合信号并根据计算不符合事件数输出错误数目NB。另外，计数器 505接收来自锁定控制器105或305的作为计数重新设置信号的锁定解除信号 S_{RL} 。另外，如图5中的实施例所示，也可从锁定解除许可部分 304接收锁定解除许可信号。选择器504根据错误的数目 N_E 来选择时钟信号 S_{T0} 到 S_{T2} 中的一个并将其作为一个许可信号 S_T 输出到核对许可部分 102 或锁定解除许可部分 304。

逻辑电路503由一个与非门 NAND1 和另一个与非门 NAND2 组成，NAND1 将计数器 502 的反向输出 Q_0 和 Q_1 作为输入,NAND2 将计数器 502 的反向输出 Q_0 和 Q_1 作为输入。与非门 NAND1 和 NAND2 将时钟信号 S_{T1} 和 S_{T2} 输出到选择器 504。计数器502的反向输出 Q_0 也被作为时钟信号 S_{T0} 被提供到选择器504。

计数器502和逻辑电路503产生多个与基准时钟信号CLK具有不同周期的时钟信号 S_{T0} 到 S_{T2} 。选择器504根据由计数器505计算出的错误数目 N_E 来选择时钟信号 S_{T0} 到 S_{T2} 中的一个。不符合信号，其作为核对部分103或302的两个比较结果中的一个被作

为时钟信号提供到计数器５０５。一个用于将许可信号生成周期设定为最小值的诸如一锁定解除信号 S_{RL} 的信号被作为重新设置信号提供到计数器 505。在此情况下，就实现了当比较结果为“符合”时在最小值设定许可信号生成间隔的功能（图２中的步骤Ｓ２０４或图６中的步骤Ｓ４０４）。

如图１０中所示，在此实例中，选择器５０４接收到从 S_{T0} 到 S_{T2} 的三种波形。当错误数目 N_E 为零时（通常状态下），一具有一给定周期的定时时钟信号 S_{T0} 被选定作为许可信号 S_T 。当错误数目 N_E 为１时，一频率减半定时时钟信号 S_{T1} 被选择作为许可信号 S_T 。当错误的数目为２时，一四分之一频率定时信号 S_{T2} 被选择作为许可信号 S_T 。简而言之，许可信号 S_T 的频率或周期根据比较结果中的不符合的事件的数目被控制。

在此实例中，因为计数器５０５为一２比特计数器从而其最大错误可数数目为３。可通过增加计数器５０５的比特的数目及由计数器５０２和逻辑电路５０３产生的信号的种类，即不同种类的频率来增加可数错误的数目。通常，具有不同因子的Ｎ个（Ｎ为整数）分频器可被用来产生具有不同频率的Ｎ个 S_{T0} -S_{TN} 的时钟信号。选择器从Ｎ个时钟信号中选择出一个作为许可信号 S_T 。另外，图９的电路结构可以很容易地通过使用公知的ＤＳＰ（数字信号处理器）、ＣＰＵ（中央处理部分）或类似的结构来完成。

如图１１中所示，用同一参考数码来表示与图９中前面所描述的类似的电路块，处理器（或逻辑电路）５０６可被用来控制基于错误数目 N_E 的选择器。例如,此结构可包含这样一种情况即错误的数目 N_E 超过某一允许范围。特别地,当错误的数目 N_E 超过一允许范围时,例如 $0 \leqslant N_E \leqslant 8$，核对操作被停止。

借助处理器５０６通过使错误的数目 N_E 和许可信号生成间隔之间的关系更复杂可生成很难被破译的密码。特别地，根据错误的数目 N_E 通过处理器５０６来产生随机数，以使得选择器５０４随机地选择时钟信号的周期。在这种情况下，由于许可信号 S_T 的频率根据随机数而随机地变化，从而变得很难来破译该密码。

虽然为了描述的方便，在以上的实施例中密码被假定为是一位数字，很明显地本发明中也可使用两位或多位的数字。在后一种情况下，本实施例可被调整为使整个的输入密码与预先存储在存储器中的整个密码进行比较。

另外，如图1中所示核对许可部分102可由延迟触发电路组成，其将许可信号 S_T 作为定时时钟使用。如图5中所示锁定解除许可部分304可由输入许可信号 S_T 和比较结果的与门组成。无需说，由核对许可部分102、核对部分103、锁定控制器105和许可信号发生器107组成的结构可通过程序可控的处理器（DSP或CPU）来完成。类似地，由核对部分302、锁定解除许可部分304、锁定控制器305和许可信号发生器307组成的结构可通过程序受控的处理器（DSP或CPU）来完成。

如上所述，根据本发明，核对操作之间的间隔或锁定解除许可操作间的间隔根据密码比较结果中的不符合事件的数目来延长。因此，即使输入所有可能的密码，也不会产生符合。这提供了一个优点，即即使使用计算机等工具也不容易破译密码。另外，根据本发明，密码输入功能不被锁定。这提供了另一个好处，即在即使输入一个错误密码后，也可通过输入一个已注册的密码来解除系统的锁定。

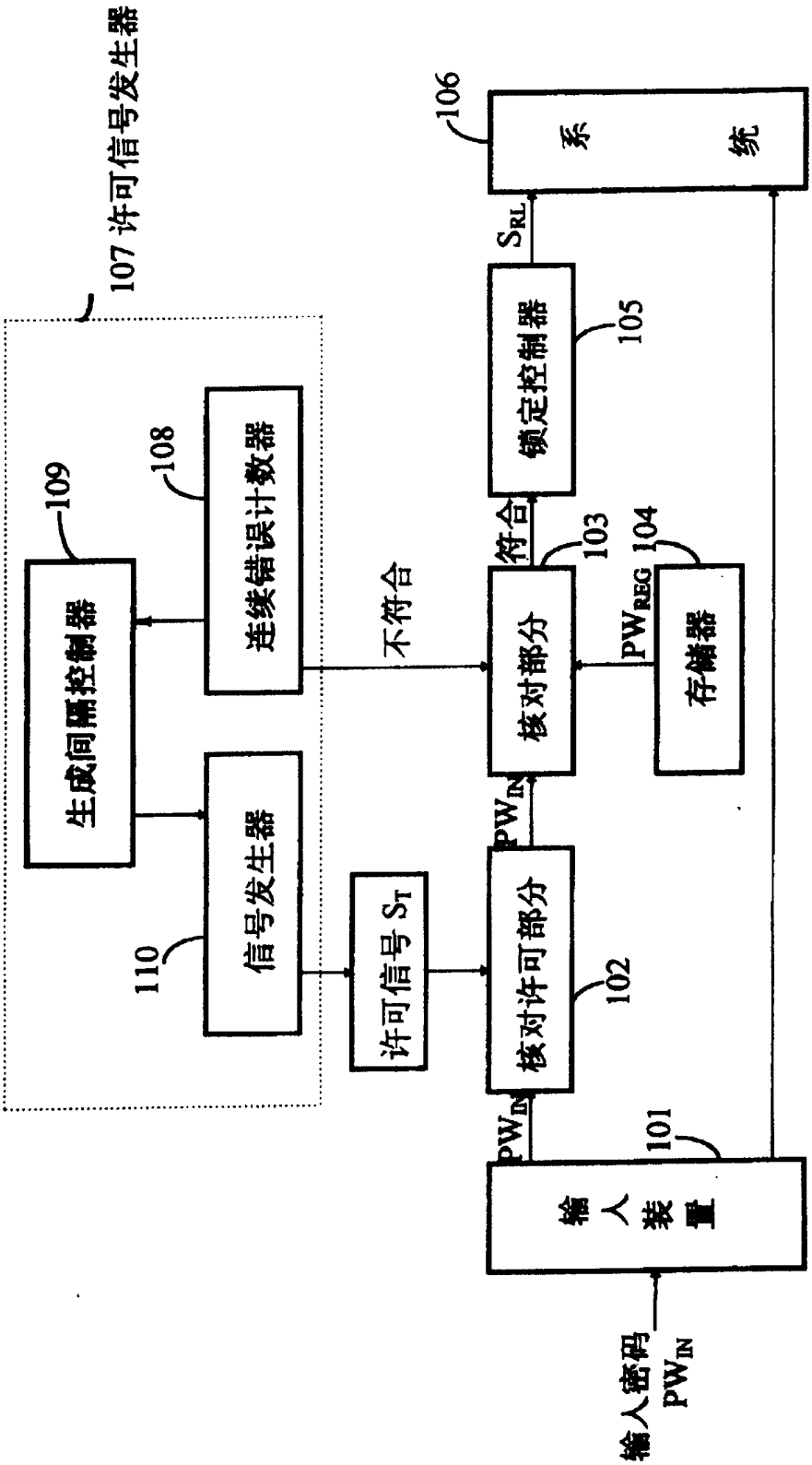

107 许可信号发生器
生成间隔控制器
109
连续错误计数器
108
信号发生器
110
许可信号 S_T
核对许可部分
102
PW_{IN}
核对部分
103
PW_{REG}
存储器
104
符合
不符合
锁定控制器
105
S_{RL}
系统
106
输入装置
101
PW_{IN}
输入密码
PW_{IN}

图 1

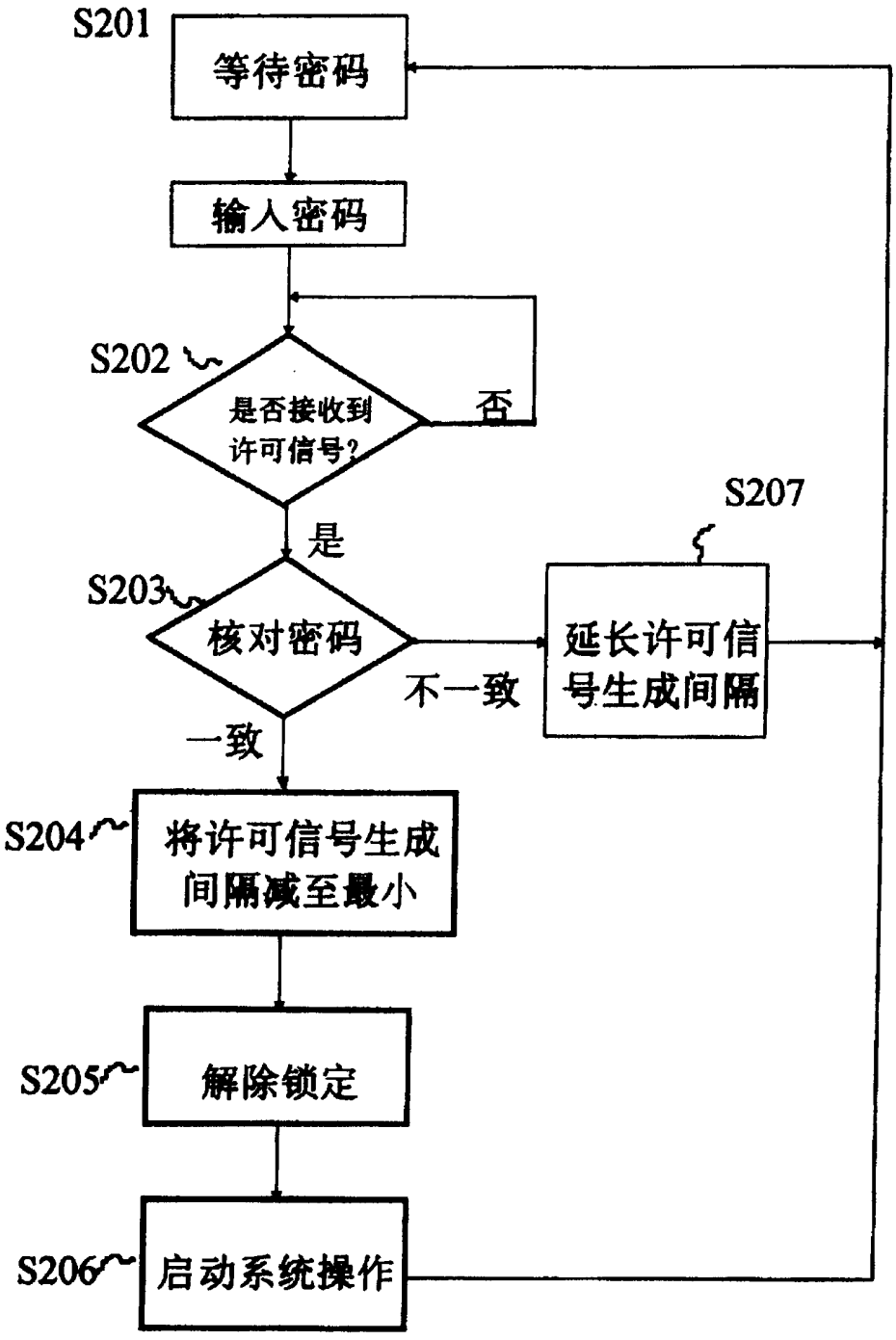

S201
等待密码
输入密码
S202
是否接收到许可信号?
否
是
S203
核对密码
不一致
S207
延长许可信号生成间隔
一致
S204
将许可信号生成间隔减至最小
S205
解除锁定
S206
启动系统操作

图 2

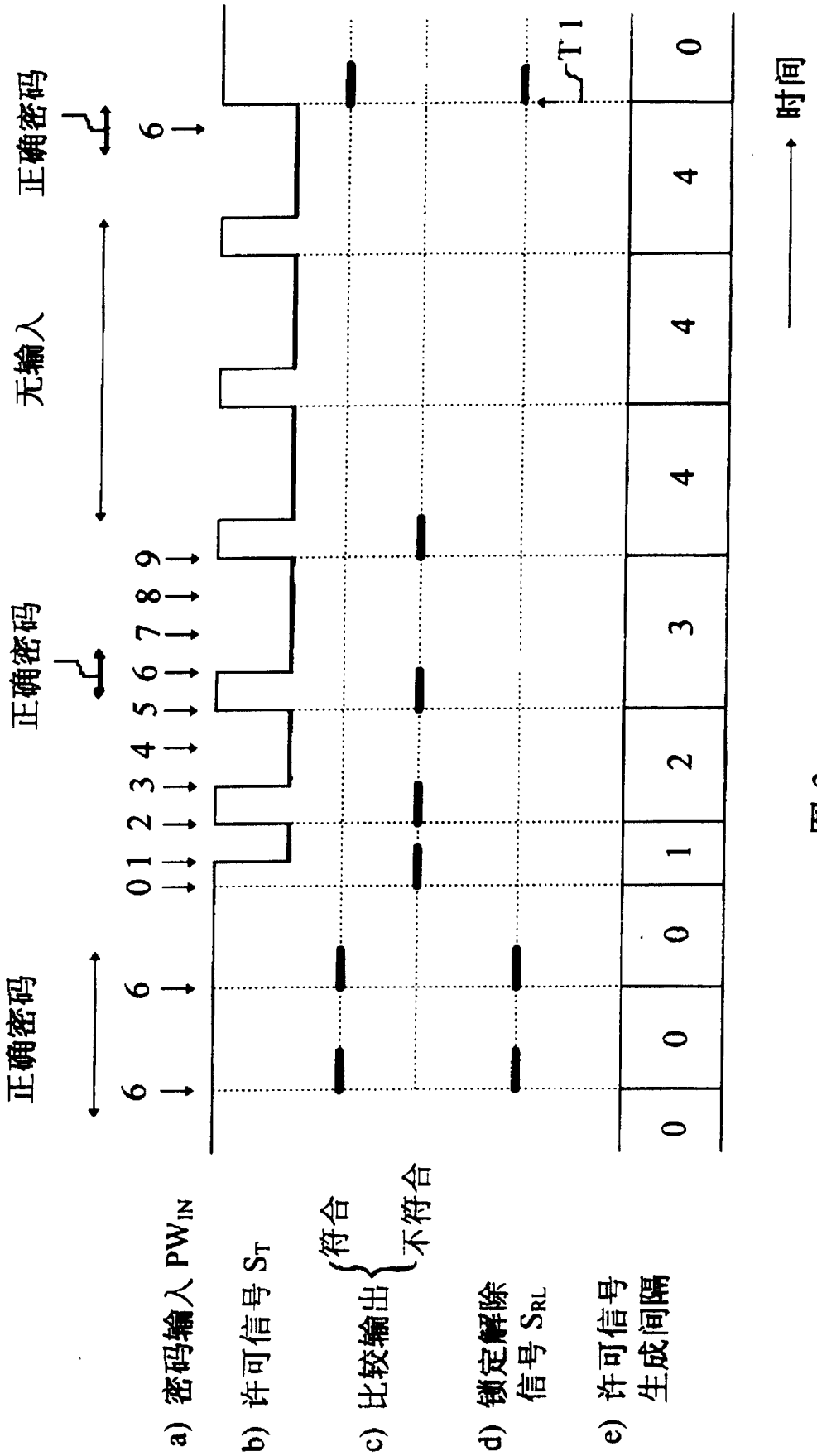

正确密码
正确密码
无输入
正确密码
6 6 0 1 2 3 4 5 6 7 8 9 6
a) 密码输入 PWIN
b) 许可信号 ST
c) 比较输出
符合
不符合
d) 锁定解除信号 SRL
e) 许可信号生成间隔
T1
0 0 0 1 2 3 4 4 4 0
时间

图 3

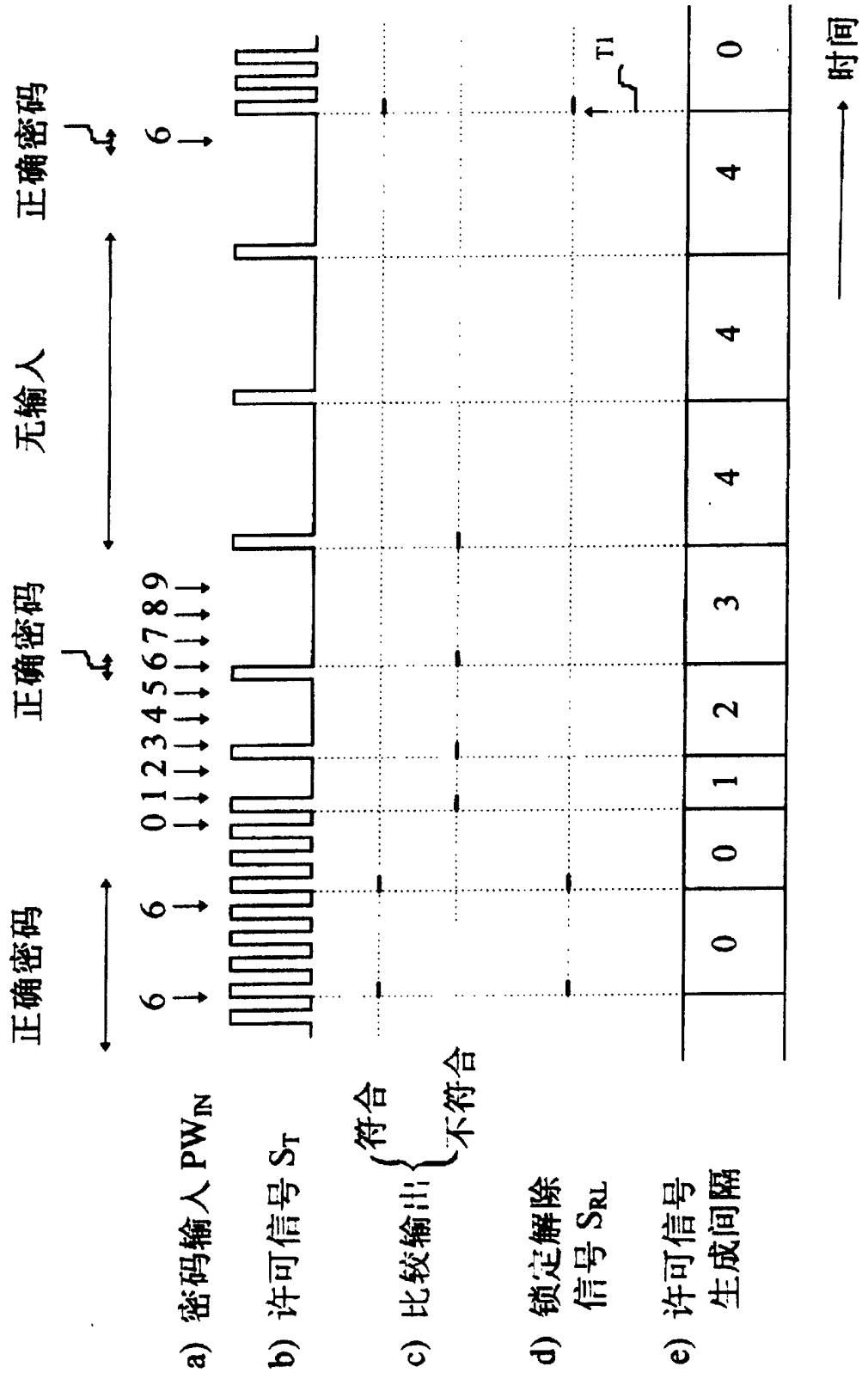

正确密码
正确密码
无输入
正确密码
6
6
6
0 1 2 3 4 5 6 7 8 9
a) 密码输入 PW_{IN}
b) 许可信号 S_T
c) 比较输出
符合
不符合
d) 锁定解除信号 S_{RL}
e) 许可信号生成间隔
T1
0
0
1
2
3
4
4
4
0
时间

图 4

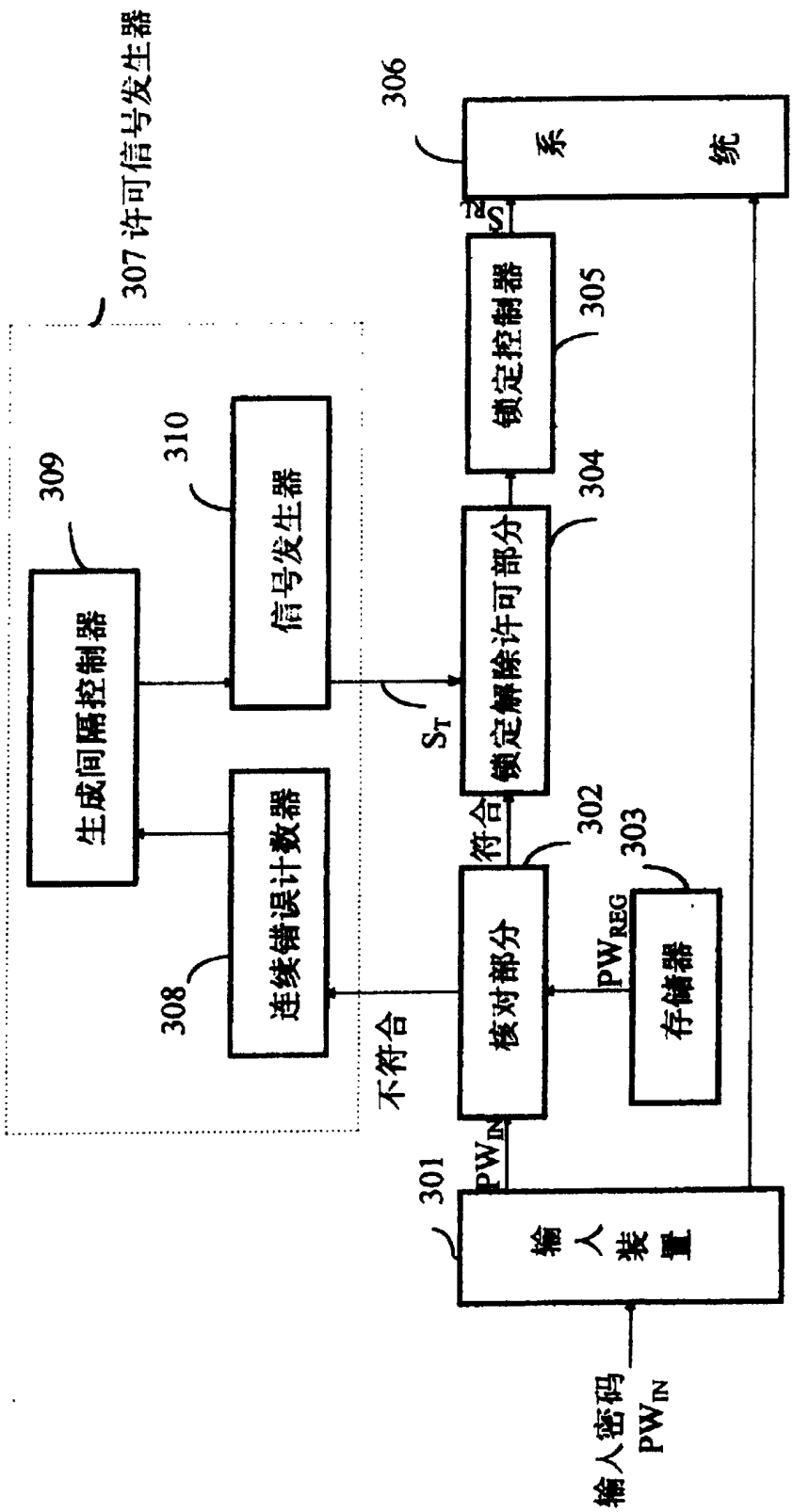

输入密码
PW_{IN}
输入装置
301
PW_{IN}
核对部分
302
PW_{REG}
存储器
303
符合
不符合
锁定解除许可部分
304
锁定控制器
305
系统
306
S_T
307 许可信号发生器
生成间隔控制器
309
信号发生器
310
连续错误计数器
308

图 5

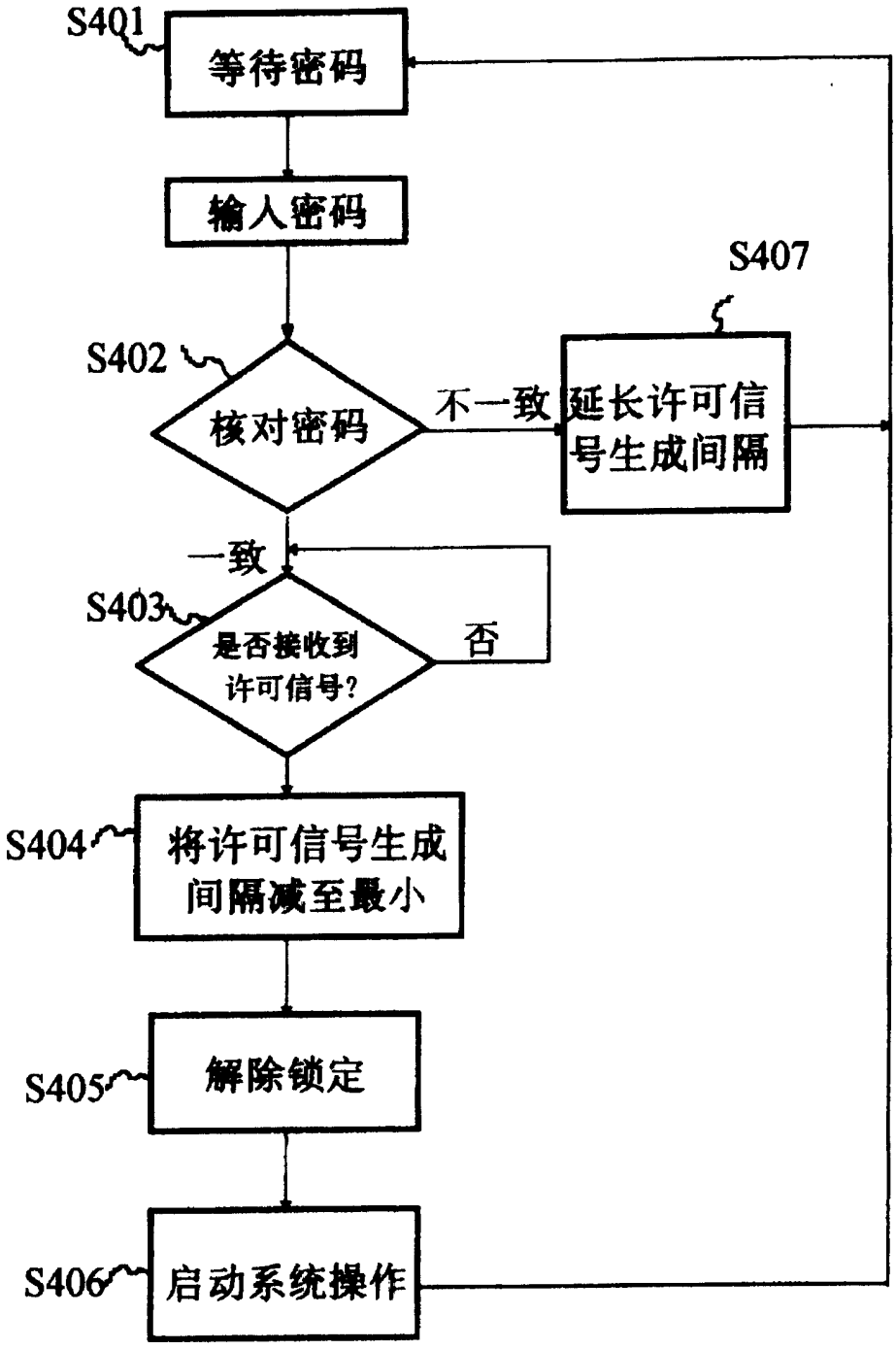

S401
等待密码
输入密码
S407
S402
核对密码
不一致
延长许可信号生成间隔
一致
S403
是否接收到许可信号?
否
S404
将许可信号生成间隔减至最小
S405
解除锁定
S406
启动系统操作

图 6

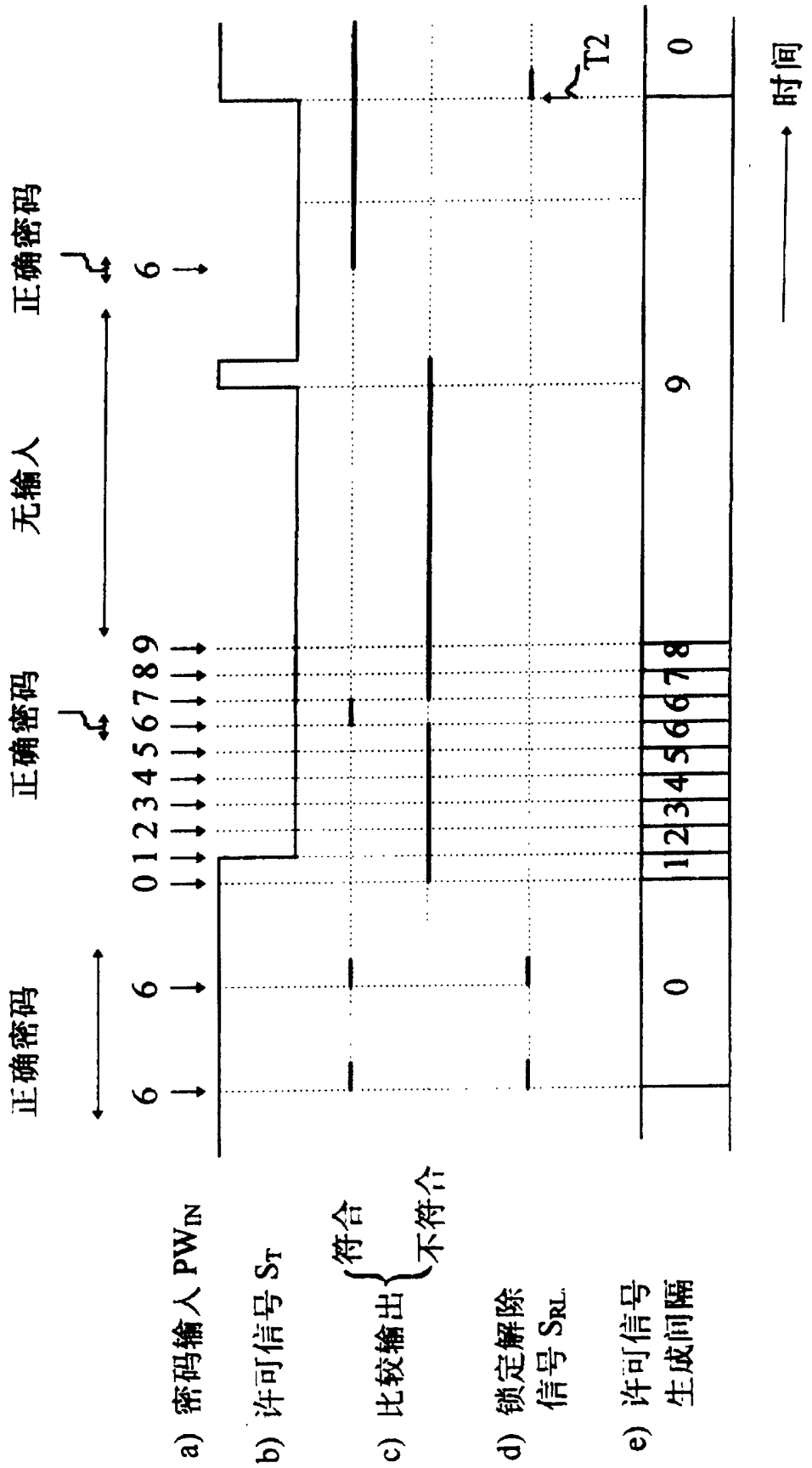

正确密码
正确密码
无输入
正确密码
6
6
0 1 2 3 4 5 6 7 8 9
6
a) 密码输入 PWIN
b) 许可信号 ST
c) 比较输出
符合
不符合
d) 锁定解除
信号 SRL
e) 许可信号
生成间隔
T2
0
1 2 3 4 5 6 7 8
9
0
时间

图 7

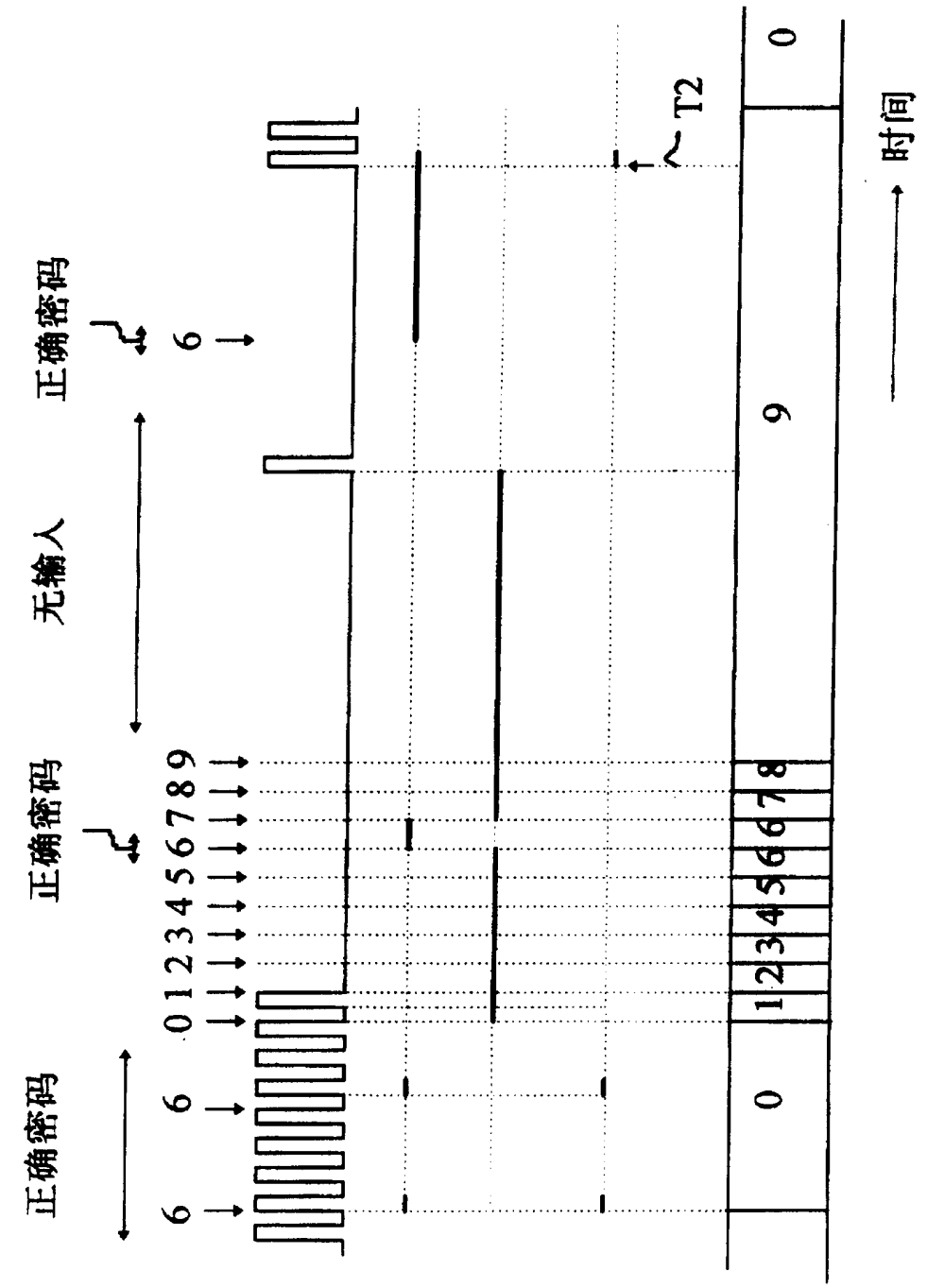

正确密码
正确密码
无输入
正确密码
6
6
6
0 1 2 3 4 5 6 7 8 9
a) 密码输入 PW_{IN}
b) 许可信号 S_T
c) 比较输出
符合
不符合
d) 锁定解除信号 S_{RL}
e) 许可信号生成间隔
T2
0
1 2 3 4 5 6 6 7 8
9
0
时间

图 8

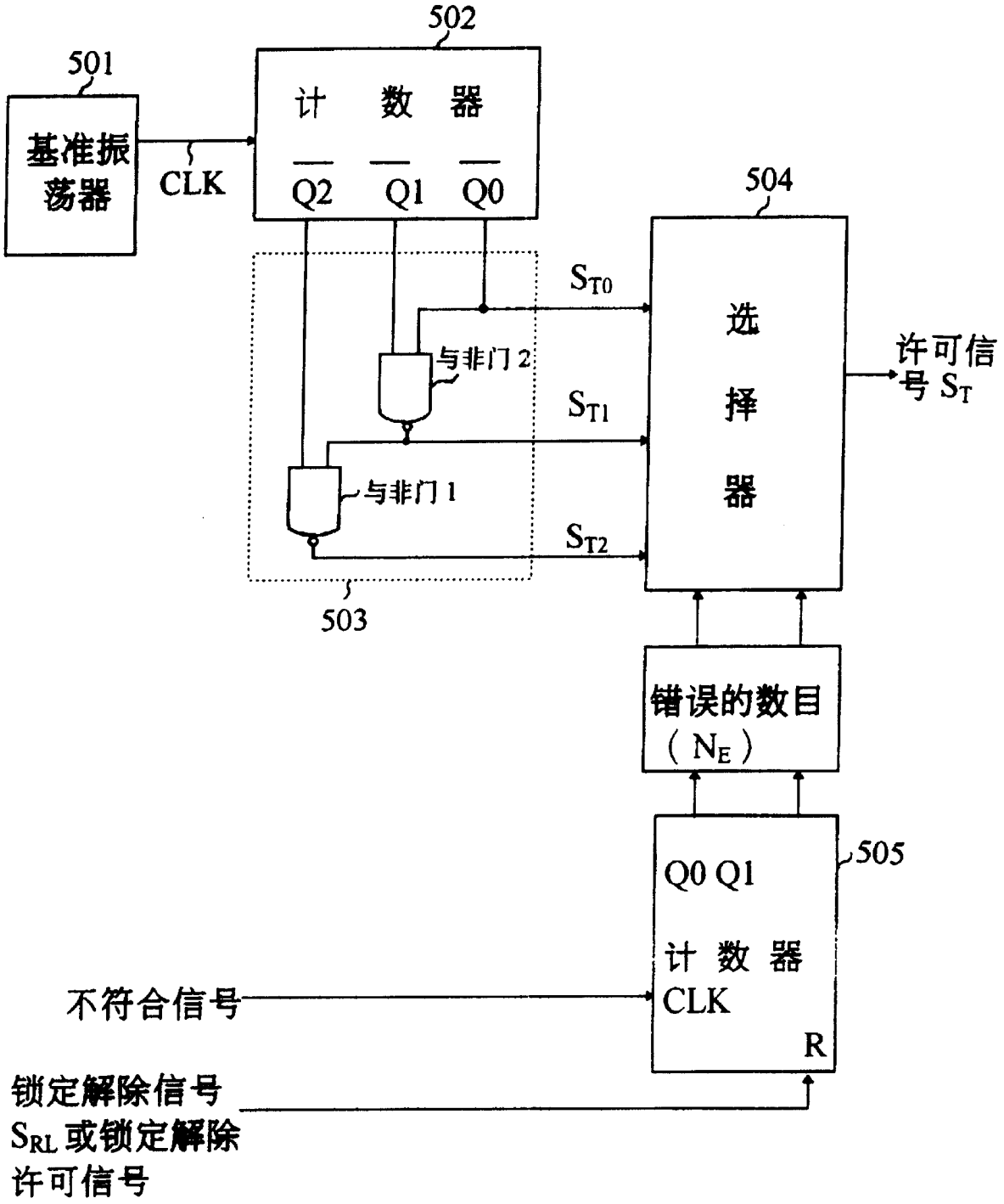

502
501
计 数 器
基准振荡器
CLK
Q2 Q1 Q0
504
S_{T0}
选
择
器
许可信号 S_T
与非门 2
S_{T1}
与非门 1
S_{T2}
503
错误的数目
（N_E）
505
Q0 Q1
计 数 器
CLK
R
不符合信号
锁定解除信号
S_{RL} 或锁定解除
许可信号

图 9

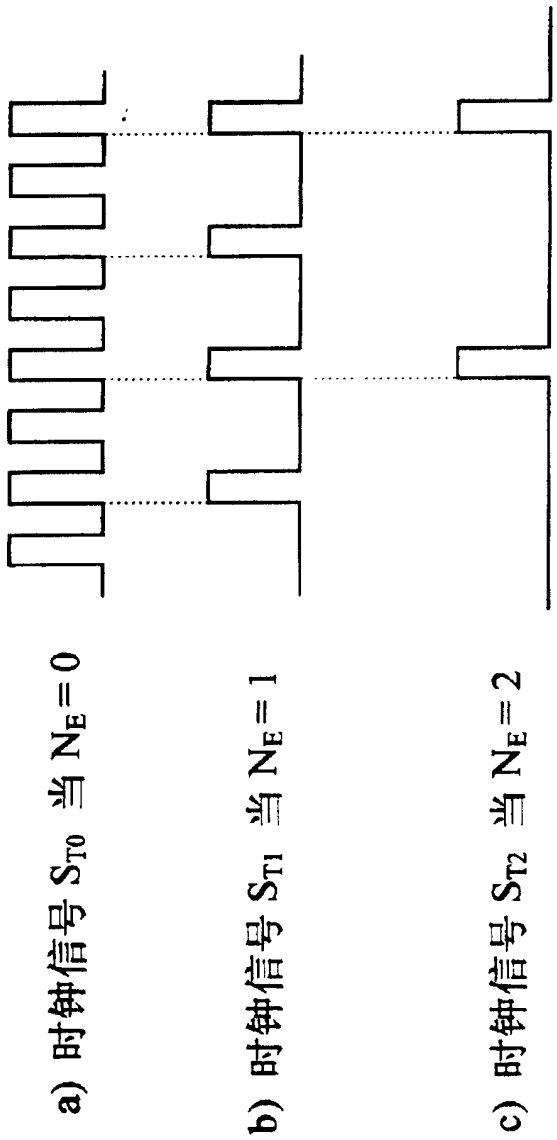


图 10

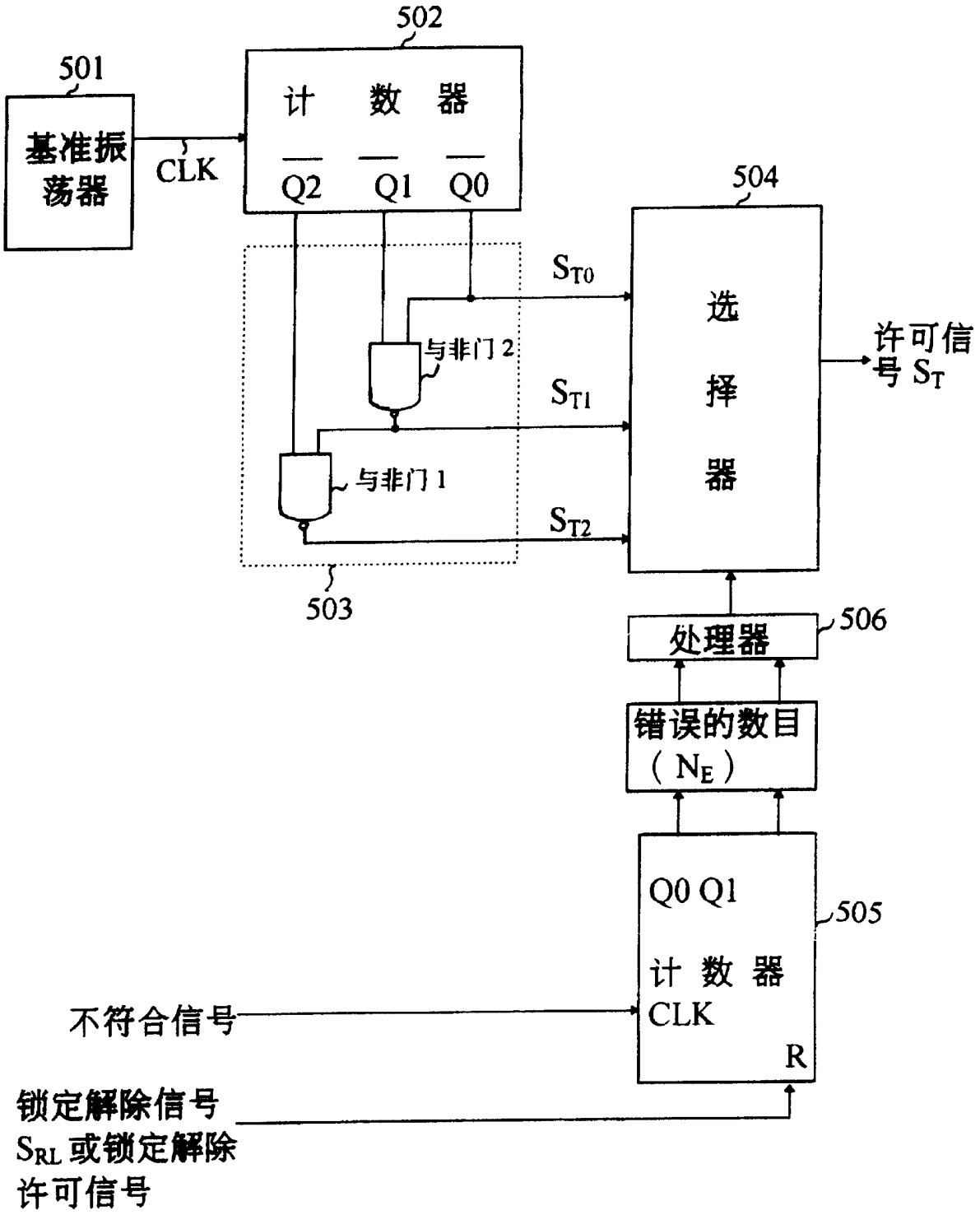

502
501
计 数 器
基准振荡器
CLK
Q2 Q1 Q0
504
S_{T0}
选
择
器
许可信号 S_T
与非门 2
S_{T1}
与非门 1
S_{T2}
503
处理器
506
错误的数目
(N_E)
Q0 Q1
505
计 数 器
CLK
R
不符合信号
锁定解除信号
S_{RL} 或锁定解除
许可信号

图 11