[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/22 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200880016028.7

[43] 公开日 2010 年 3 月 24 日

[11] 公开号 CN 101681415A

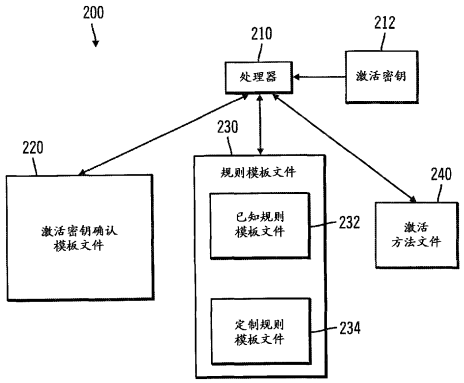
[22] 申请日 2008.5.27
[21] 申请号 200880016028.7
[30] 优先权
[32] 2007. 6.18 [33] US [31] 11/764,547
[86] 国际申请 PCT/EP2008/056507 2008.5.27
[87] 国际公布 WO2008/155198 英 2008.12.24
[85] 进入国家阶段日期 2009.11.13
[71] 申请人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 B·R·莫德西特
[74] 专利代理机构 北京市金杜律师事务所
代理人 王茂华
权利要求书 4 页 说明书 14 页 附图 8 页

[54] 发明名称

用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译所述数字内容的方法和设备

[57] 摘要

一种用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的方法和装置。 用于确认激活密钥的规则、提供在执行用于确认激活密钥的规则时使用的指令的代码以及用于标识可能的激活密钥的模板被分离并独立保护，其中所述密钥是当前有效的，并且确认与每个当前有效的激活密钥相关联的规则。



1. 一种处理设备可读的程序存储设备，包括:

所述处理设备可执行的程序指令，用以执行提供用于数字内容的功能的激活密钥的操作，所述操作包括:

提供标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的非加密文件;

提供定义用于确认每个所述激活密钥的规则的非加密文件;

提供在执行适于确认每个所述激活密钥的所述规则时使用的代码指令的文件；以及

至少对标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的所述非加密文件进行加密。

2. 根据权利要求 1 所述的程序存储设备，其中所述提供标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的非加密文件还包括:

提供包括以下各项的平面文件:激活密钥的列表，激活密钥的描述，关于激活密钥是否有效的指示，以及关于用于验证每个激活密钥的确认规则的指示。

3. 根据权利要求 1 所述的程序存储设备，其中至少对标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的所述非加密文件进行加密还包括:

对定义所述规则的文件以及所述代码指令的文件进行加密。

4. 根据权利要求 1 所述的程序存储设备，其中所述提供定义用于确认每个所述激活密钥的规则的文件还包括:

预先确定确认每个所述激活密钥的所述规则，使得不必修改定义所述规则的文件和用于执行所述规则的代码便可实现新的激活密钥。

5. 根据权利要求 1 所述的程序存储设备，还包括:

提供用于在标识用于实现数字内容的相关功能的激活密钥、且标

识适于确认每个所述激活密钥的规则的非加密文件与标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个所述激活密钥的规则的文件的二进制加密版本之间进行转换的代码。

6. 根据权利要求 1 所述的程序存储设备，其中所述提供用于在标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个所述激活密钥的规则的非加密文件与二进制加密版本之间进行转换的代码还包括：

仅编写用于转换的所述代码一次。

7. 一种用于提供用于数字内容的功能的激活密钥的系统，包括：

标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的加密文件；

定义用于确认每个激活密钥的规则的加密文件；以及

在执行适于确认每个所述激活密钥的所述规则时使用的代码指令的文件。

8. 根据权利要求 7 所述的系统，其中所述标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的加密文件还包括包含以下内容的文件：激活密钥列表，激活密钥的描述，关于激活密钥是否有效的指示，以及关于用于验证每个激活密钥的确认规则的指示。

9. 根据权利要求 7 所述的系统，其中定义用于确认每个所述激活密钥的所述规则的所述加密文件还包括：

用于确认每个所述激活密钥的、预先创建的规则，使得不必修改定义所述规则的文件和用于执行所述规则的代码便可实现新的激活密钥。

10. 根据权利要求 7 所述的系统，还包括：

用于将标识激活密钥且标识适于确认每个所述激活密钥的所述规则的非加密文件转换为标识激活密钥且标识适于确认每个所述激活密钥的所述规则的所述加密文件的代码。

11. 根据权利要求 7 所述的系统，其中所述规则模板文件还包括：

已知规则模板文件和定制规则模板文件。

12. 根据权利要求 7 所述的系统，其中所述规则模板文件还包括：

用于确认激活密钥的算法。

13. 根据权利要求 7 所述的系统，其中用于确认激活密钥的所述算法仅开发一次。

14. 一种用于提供用于数字内容的功能的激活密钥的方法，包括：

提供标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的非加密文件；

提供定义用于确认每个所述激活密钥的所述规则的非加密文件；

提供在执行适于确认每个所述激活密钥的所述规则时使用的代码指令的文件；以及

至少对标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的所述非加密文件进行加密。

15. 根据权利要求 14 所述的方法，其中所述提供标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的非加密文件还包括：

提供包含如下内容的平面文件：激活密钥列表，激活密钥的描述，关于激活密钥是否有效的指示，以及关于用于验证每个激活密钥的确认规则的指示。

16. 根据权利要求 14 所述的方法，其中所述至少对标识用于实现数字内容的相关功能的激活密钥，且标识适于确认每个所述激活密钥的规则的所述非加密文件进行加密还包括：

对定义所述规则的文件以及所述代码指令的文件进行加密。

17. 根据权利要求 14 所述的方法，其中所述提供定义用于确认每个所述激活密钥的所述规则的文件还包括：

预先确定确认每个所述激活密钥的所述规则，使得不必修改定义所述规则的文件和用于执行所述规则的代码便可实现新的激活密钥。

18. 根据权利要求 14 所述的方法，还包括：

提供用于在标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个所述激活密钥的规则的非加密文件与标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个所述激活密钥的所述规则的文件的二进制加密版本之间进行转换的代码。

19. 根据权利要求 14 所述的方法，其中所述提供用于在标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个所述激活密钥的规则的所述非加密文件与二进制加密版本之间进行转换的代码还包括:

仅编写用于转换的所述代码一次。

20. 一种可加载到数字计算机内存中的计算机程序产品，包括软件代码部分，用于当所述产品在计算机上运行时实现根据权利要求 14 至 19 所述的发明。

用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译所述数字内容的方法和设备

技术领域

本发明总体上涉及正如软件的数字内容的安全特征，且更具体地，涉及用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译所述数字内容的方法和设备。

背景技术

软件产品的创建和销售为具有创新产品的公司创造了巨大的财富。可将计算系统制造为具有默认为禁止的一个或多个特征。词语“特征”指代提供（或增强）特定功能的计算机组件。“计算系统”指代各种各样处理数字化信息的设备，例如，桌面计算机、膝上型计算机、服务器、网络基础设施设备（例如，路由器、交换机等）、数字家庭娱乐系统、蜂窝电话等。

默认地禁止特征的一个原因是为计算机（或其组件）提供升级路径。例如，很多软件程序被设计为允许用户最初获得程序的简单版本并随后将该简单版本升级为更鲁棒的版本。在某些情况下，程序的两个（或更多）版本间的差异仅仅是程序的哪些特征被禁止的问题。程序的简单版本可能以较低的价格销售，反映出并非所有特征都可用。

想要升级软件的用户可从例如软件厂商处购买对更鲁棒版本的访问。通常，软件厂商不需要向升级软件的用户发送新的软件模块。原因是，通常，支持更鲁棒特征的代码已经在程序中，但是此代码被禁止。为了启用软件特征，厂商可提供能够使附加软件特征被激活的激活密钥。

因此，激活密钥（或称激活码）可用于启用在顾客为该特征付

费之后可自动激活的特征。然而，相当常见的是，用于新软件功能的附加激活密钥类型必须被添加到软件产品中。目前，添加激活密钥类型需要针对每个新功能的每个新密钥类型而改变代码。而且，在产品出厂之前，很多时候是在最后时刻，激活码的参数可能改变，这导致最后时刻对代码的修改。当激活码改变或添加激活密钥码时，必须花费时间在代码开发上。这时，存在使代码出错的风险。而且，相当大量的时间花费在了测试这种代码改变上。

为了克服代码修改带来的问题，可以创建平面文件，该文件中具有确认特定激活密钥类型的所需信息。平面文件是包含不具有结构化关系的记录的文件。需要附加的知识来解释这些文件，如文件格式属性。平面文件只能被顺序地读或写，但是其包括一个或更多记录。但是，使用平面文件是有问题的，因为任何人在任何时间都可以修改平面文件。这会允许某些人在没有进行适当检查的情况下就对激活密钥进行激活，或者可能允许某些人在激活密钥所启用的其余底层代码尚不可用时便激活密钥。

可以看出，需要一种用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的方法和设备。

发明内容

为了克服上述现有技术的限制，以及克服当阅读和理解本说明书时变得易见的其他限制，本发明的实施例包括用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的方法和设备。

本发明的实施例对用于确认激活密钥的规则、用于提供执行用于确认激活密钥的规则的指令的代码以及用于标识可能激活密钥的模板进行了分离，其中所述密钥目前是有效的，并且确认与每个当前有效的激活密钥相关联的规则。因此，针对每个新功能的每个新密钥类型的代码改变以及激活码的参数的改变不需要用于代码开发

的附加时间，并且因此消除了在产品即将出厂前造成的错误。此外，花费在测试代码修改上的时间可以整合到开发周期中，而不是添加到产品出厂前的最后时刻，由此消除了由这种代码改变引起的产品延期。

在本发明的一个实施例中，提供了一种处理设备可读的程序存储设备。所述程序存储设备包括处理设备可执行的程序指令，用以执行提供用于数字内容的功能的激活密钥的操作。所述操作包括：提供标识用于实现数字内容的相关功能的激活密钥且标识适于确认每个激活密钥的规则的非加密文件；提供定义用于确认每个激活密钥的规则的非加密文件；提供在执行适于确认每个激活密钥的规则时使用的代码指令的文件；以及至少对标识用于实现数字内容的相关功能的激活密钥且标识适于确认每个激活密钥的规则的非加密文件进行加密。

优选地，本发明提供了一种程序存储设备，其中，提供标识用于实现数字内容的相关功能的激活密钥且标识适于确认每个激活密钥的规则的非加密文件还包括提供包括以下内容的平面文件：激活密钥的列表，激活密钥的描述，关于激活密钥是否有效的指示，以及关于用于验证每个激活密钥的确认规则的指示。

优选地，本发明提供了一种程序存储设备，其中，至少对标识用于实现数字内容的相关功能的激活密钥且标识适于确认每个激活密钥的规则的非加密文件进行加密还包括：对定义规则的文件以及代码指令的文件进行加密。

优选地，本发明提供了一种程序存储设备，其中，提供定义用于确认每个激活密钥的规则的文件还包括：预先确定确认每个激活密钥的规则，使得不必修改定义规则的文件和用于执行该规则的代码便可实现新的激活密钥。

优选地，本发明提供了一种程序存储设备，还包括：提供用于在标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件与标识用于实现数字内容的相关

功能的激活密钥、且标识适于确认每个激活密钥的规则的文件的二进制加密版本之间进行转换的代码。

优选地，本发明提供了一种程序存储设备，其中，提供用于在标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件与二进制加密版本之间进行转换的代码还包括：仅编写该用于转换的代码一次。

在本发明的另一实施例中，提供了另一种处理设备可读的程序存储设备。所述程序存储设备包括处理设备可执行的程序指令，用以执行用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的操作。所述操作包括：确定激活密钥的参数和属性；标识用于确认激活密钥的算法；创建非加密的激活密钥确认模板文件；提供用于将非加密的激活密钥确认模板文件转换为二进制加密版本且用于确认激活密钥的代码；创建非加密的已知规则模板文件并将所述非加密的已知规则模板文件转换为二进制加密已知规则模板文件；创建非加密的定制规则模板文件并将所述非加密的定制规则模板文件转换为二进制加密定制规则模板文件；提供非加密的激活方法文件并将所述非加密的激活方法文件转换为二进制加密激活方法文件；当需要新的激活密钥类型时，修改非加密的激活密钥确认模板文件并将修改后的非加密的激活密钥确认模板文件转换为二进制加密激活密钥确认模板文件；以及当需要新的定制确认规则时，修改非加密的定制规则模板文件并将修改后的非加密的定制规则模板文件转换为二进制加密定制规则模板文件。

在本发明的另一实施例中，提供了一种提供用于数字内容的功能的激活密钥的系统。所述系统包括：标识用于实现数字内容的相关功能的激活密钥且标识适于确认每个激活密钥的规则的加密文件；定义用于确认每个激活密钥的规则的加密文件；在执行适于确认每个激活密钥的规则时使用的代码指令的文件。

优选地，本发明提供了一种系统，其中，标识用于实现数字内容的相关功能的激活密钥且标识适于确认每个激活密钥的规则的加

密文件还包括包含以下内容的文件：激活密钥的列表，激活密钥的描述，关于激活密钥是否有效的指示，以及关于用于验证每个激活密钥的确认规则的指示。

优选地，本发明提供了一种系统，其中，定义用于确认每个激活密钥的规则的加密文件还包括：用于确认每个激活密钥的、预先创建的规则，使得不必修改定义规则的文件和用于执行该规则的代码便可实现新的激活密钥。

优选地，本发明提供了一种系统，还包括：用于将标识激活密钥且标识适于确认每个激活密钥的规则的非加密文件转换为标识激活密钥且标识适于确认每个激活密钥的规则的加密文件的代码。

优选地，本发明提供了一种系统，其中，规则模板文件还包括：已知规则模板文件和定制规则模板文件。

优选地，本发明提供了一种系统，其中，规则模板文件还包括：用于确认激活密钥的算法。

优选地，本发明提供了一种系统，其中，用于确认激活密钥的算法仅开发一次。

在本发明的另一实施例中，提供了一种提供用于数字内容的功能的激活密钥的方法。所述方法包括：提供标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件；提供定义用于确认每个激活密钥的规则的非加密文件；提供在执行适于确认每个激活密钥的规则时使用的代码指令的文件；以及至少对标识用于实现数字内容的相关功能的激活密钥且标识适于确认每个激活密钥的规则的非加密文件进行加密。

在本发明的另一实施例中，提供了一种提供用于数字内容的功能的激活密钥的方法。所述方法包括步骤：提供标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件；提供定义用于确认每个激活密钥的规则的非加密文件；提供在执行适于确认每个激活密钥的规则时使用的代码指令的文件；以及至少对标识用于实现数字内容的相关功能的激活密钥且

标识适于确认每个激活密钥的规则的非加密文件进行加密。

优选地，本发明提供了一种方法，其中提供标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件还包括提供包括以下内容的平面文件：激活密钥的列表，激活密钥的描述，关于激活密钥是否有效的指示，以及关于用于验证每个激活密钥的确认规则的指示。

优选地，本发明提供了一种方法，其中至少对标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件进行加密还包括：对定义规则的文件以及代码指令的文件进行加密。

优选地，本发明提供了一种方法，其中，提供定义用于确认每个激活密钥的规则的文件还包括：预先确定确认每个激活密钥的规则，使得不必修改定义规则的文件和用于执行该规则的代码便可实现新的激活密钥。

优选地，本发明提供了一种方法，还包括：提供用于在标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件与标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的文件的二进制加密版本之间进行转换的代码。

优选地，本发明提供了一种方法，其中，提供用于在标识用于实现数字内容的相关功能的激活密钥、且标识适于确认每个激活密钥的规则的非加密文件与二进制加密版本之间进行转换的代码还包括：仅编写该用于转换的代码一次。

在另一实施例中，本发明提供了一种可加载到数字计算机内存中的计算机程序产品，包括软件代码部分，用于当所述产品在计算机上运行时实现如上所述的本发明。

描述本发明的实施例的特征的这些和各种其他优点和新特性用此处所附权利要求中的特殊性指出并形成其一部分。但是，为了更好地理解本发明的实施例、其优点以及通过其使用获得的目的，应

该参考形成这里另一部分的附图以及所附的描述内容，其中示出和描述了本发明的特定实施例。

附图说明

现在将参考附图仅通过举例说明本发明的实施例，其中：

图 1 示出了根据本发明优选实施例的系统；

图 2 示出了根据本发明优选实施例的用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的系统；

图 3 示出了根据本发明优选实施例的激活密钥确认模板文件；

图 4a-图 b 示出了为根据本发明优选实施例的用于标识确认激活密钥的算法的规则模板文件；

图 5 示出了根据本发明优选实施例的激活方法文件；

图 6 是根据本发明优选实施例的用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的方法的流程图；

图 7 示出了根据本发明优选实施例的改变激活密钥确认模板文件的示例；

图 8 示出了根据本发明优选实施例的利用新的定制确认规则改变激活密钥确认模板文件的示例。

具体实施方式

在对实施例的下文描述中将参考形成其一部分的附图，其中通过示例的方式示出了可以实现本发明的特定实施例。应理解可使用其他实施例，因为可以进行结构上的改变而不脱离本发明实施例的范围。

本发明的实施例提供了一种用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的方法和设备。二进制加密模板文件被用来确认激活密钥类型。二进制加密模板文件防止未授权的用户访问和改变确认模板文件。二进制加密规则模板文

件还被用来指示检查的功能，使得在需要添加新的检验方法时不必编写代码。提供二进制加密激活方法文件，用以指示代码如何对激活密钥进行激活。

图 1 示出了根据本发明实施例的系统 100。本发明的实施例可采用完全的软件实施例或包含硬件和软件元件的实施例的形式。在一个优选实施例中，本发明实现在软件中，包括但不限于固件、驻留软件、微码等。而且，本发明的实施例可采用计算机可用或计算机可读介质 168 可访问的计算机程序产品 190 的形式，提供被计算机或任何指令执行系统使用或与其一起使用的程序代码。

为了此描述的目的，计算机可用或计算机可读介质 168 可以是任何可包含、存储、传递、传播或传输被指令执行系统、装置或设备使用或与其一起使用的程序的装置。介质 168 可以是电子的、磁的、光的、电磁的、红外的或半导体系统（或装置或设备）或传播介质。计算机可读介质的示例包括半导体或固态存储器、磁带、可移除计算机盘、随机存取存储器（RAM）、只读存储器（ROM）、硬磁盘和光盘。当前光盘的示例包括压缩盘-只读存储器（CD-ROM）、压缩盘-读/写（CD-R/W）和 DVD。

适合存储和/或执行程序代码的系统包括通过系统总线 120 直接或间接耦合到存储器元件 192 的至少一个处理器 196。存储器元件 192 可包括在程序代码实际执行期间使用的局部存储器、大容量存储和提供对至少一些程序代码的暂时存储以减少在执行期间必须从大容量存储检索代码的次数的高速缓冲存储器。

输入/输出或 I/O 设备 130（包括但不限于，键盘、显示器、点击设备等）可直接地或通过中间 I/O 控制器耦合到系统。网络适配器 150 也可耦合到系统以使系统能耦合到其他系统。

因此，计算机程序 190 包括指令，当该指令被图 1 的系统 100 读和执行时，使系统 100 完成执行本发明的步骤或元件所需的步骤。

用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的本发明的实施例包括分离的加密文件。二进制

加密确认模板文件可用于确认特定的激活密钥类型。二进制加密规则模板文件指示检查功能，使得在需要添加新的检验方法时不必编写代码。而且，使用二进制加密激活方法文件来指示代码如何对激活密钥进行激活。

在创建激活密钥确认模板文件时，确定文件所需的参数和属性。激活密钥确认模板文件标识什么激活密钥类型是有效的，以及什么标识符与每个密钥类型相关联。激活密钥确认模板文件还标识哪些密钥类型是未来候选但是尚不被允许的。相同的密钥类型编号将被加密在激活密钥中，使得激活密钥可以与确认模板文件中的密钥类型号相关联。

图 2 示出了根据本发明实施例的用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的系统 200。处理器 210 访问激活密钥确认模板文件 220，以标识与所提供的激活密钥 212 相关联的参数和属性。激活密钥确认模板文件 220 可以提供激活密钥的描述、关于所提供的激活密钥是否有效的指示以及与所提供的激活密钥相关联的确认规则的标识等。处理器 210 继而可以检验规则模板文件 230，以标识用于执行确认提供的激活密钥 212 的动作。规则模板文件 230 可以包括已知规则模板文件 232 和定制模板文件 234。一旦标识了用于确认所提供的激活密钥 212 的激活规则，便访问激活方法文件 240，以执行与处理器在检验规则模板文件 230 时所标识的确认规则相关联的过程。

图 3 示出了根据本发明实施例的激活密钥确认模板文件 300。例如，激活密钥类型 310 可以是 0x1 312、0x2 314、0x3 316 和 0x4 318。但是，可能仅 0x1 312 和 0x2 314 是被允许的密钥，而 0x3 316 和 0x4 318 将在未来被允许。为每个激活密钥 312-318 提供激活密钥描述 320。所以在这种情况下，0x1 312、0x2 314、0x3 316 和 0x4 318 可被添加到确认模板文件 300，以及仅为 0x1 312 和 0x2 314 标记有效位 330。激活密钥之一将具有在其中加密的 0x1 312，而另一激活密钥将具有在其中加密的 0x1 314。并非每个字段都必须在确认模板文

件中具有值，一些可以是空白的，而模板文件仍将工作。模板文件300的ASCII版本可以转换为二进制加密版本，从而为激活密钥确认模板文件300提供唯一的安全等级。

对于每个激活密钥类型，例如0x1 312、0x2 314、0x3 316和0x4 318，激活密钥确认模板文件300包括用于每个确认规则340-370的列，其可被标记以标识特定的确认规则是否与激活密钥有关。可以根据需要向激活密钥确认模板文件300添加附加信息。某些附加信息（虽然未在图3中示出）可以包括：保存已安装的激活密钥的二进制加密文件中的激活密钥的开始字节，或二进制加密已安装激活密钥文件中的结束字节。

模板文件的ASCII版本的这个示例以表格格式示出，从而使其较为易读，但是模板文件不会物理地具有表格格式中的行。在图3中，激活密钥类型0x1 312和0x2 314是列330中指示的有效激活密钥类型，而激活密钥类型0x3 316和0x4 318在列330中当前未标记为有效。但是，未来可改变0x1 312、0x2 314、0x3 316和0x4 318的有效性。激活密钥类型0x1 312和0x2 314二者示出标记342、344，其指示激活规则1用于确认。激活密钥类型0x2 314示出标记352，其指示确认规则2也用于确认激活密钥类型0x2 314，而激活密钥类型0x1 312将不使用确认规则2 350。用于确认规则3 360的列包括标记362、364，其指示确认规则3用于确认激活密钥类型0x1 312和0x2 314。激活密钥类型0x2 314示出标记372，其指示确认规则4也用于确认激活密钥类型0x2 314，而激活密钥类型0x1 312将不使用确认规则4 370。

图4a-图4b示出了根据本发明实施例的标识用于确认激活密钥的算法的规则模板文件400。确认规则被预先确定，使得代码不必为每个未来的激活密钥类型而修改，或是被添加到规则模板文件400。使用确认规则来检查该激活密钥或其上正在安装该激活密钥的计算机系统的特定属性。

如图4a-图4b所示，规则模板文件400提供关于什么需要确认

的信息。首先开发规则模板文件 400 的 ASCII 版本。规则模板文件的 ASCII 版本稍后被转换为二进制加密版本，从而为规则模板文件 400 提供安全等级。

如图 4a-图 4b 所示，可以提供至少两类规则模板文件 400。第一类型提供当前已知的规则 410。第二类型的规则模板文件是未来将确定或定制的规则 420。二进制加密已知规则模板文件 410 提供确认规则编号 412 和确认规则描述 414。随着新规则被开发，二进制加密定制规则模板文件 420 提供确认规则编号 422 和规则确认信息。定制规则确认模板文件 420 包括确认规则的描述 424。

图 4b 中的定制规则模板文件 420 示出了定制确认规则 5 440 的参数。为定制确认规则 5 440 提供了规则描述 424。在图 4b 中，定制确认规则 5 440 的规则描述 424 是“模型 123”442。定制规则模板文件 420 标识要检查的项 426。在图 4b 中，定制确认规则 5 440 的要检查的项 426 是“模型”444。定制规则模板文件 420 还标识检查值 428。在图 4b 中，定制确认规则 5 440 的检查值 428 是“123”446。定制规则模板文件 420 继而标识当动作通过检查时要执行的动作 430。在图 4b 中，当动作通过检查时要执行的动作 430 是显示“确认已通过”448。定制规则模板文件 420 还标识当动作失败时要执行的动作 432。在图 4b 中，当动作通过检查时要执行的动作 432 是显示“确认错误－错的模型”450。

定制规则模板文件 420 还可包括不同的或附加的参数、检查值、描述、资源管理器动作、调用函数、要调用的可执行程序、要检查以确定确认过程是通过还是失败的事项等等。传递给函数的参数也可以在定制规则确认模板文件 420 中提供。此外，来自资源管理器、函数调用、可执行程序或检查的预期返回码可以在定制规则模板文件 420 中提供。例如，大多数时间返回码可以是 0，但是在某些情况下，它可以是 2。

执行检查的一个附加示例是检查激活密钥的长度，并且该长度将在模板中提供，例如 16 字节。确认规则和参数的其他示例可以包

括：检查是否安装了默认激活码，激活码对于其上将安装它的硬件序列号而言是否正确，激活密钥对于固定的块、CKD 或二者是否有效，是否达到了最大容量等等。但是，本领域技术人员将会认识到，本发明的实施例不是要限制于此处给出的示例。相反，本领域技术人员将会认识到，可以实现其他规则、参数、例程、可执行程序、属性等，而不脱离本发明的实施例的范围。

图 5 示出了根据本发明实施例的激活方法文件 500。例如函数、命令、可执行程序的代码 510 可以在激活方法文件中提供，以允许激活与所提供的激活密钥相关联的功能。代码 510 还在激活密钥确认规则的平面文件版本与相同文件的二进制加密版本之间进行转换。对文件进行转换的已编译可执行程序通常将只必须写一次，且不必为未来的激活密钥类型而修改。代码 510 将被修改一次，以便能够读取和解密激活密钥确认模板文件，并基于规则模板文件中的规则来执行必需的确认。

创建激活方法文件 500 的 ASCII 版本，其指示代码进行什么操作来激活激活密钥。在图 5 中，激活方法文件 500 的 ASCII 版本指示要调用哪个函数、命令或可执行程序 510 来激活激活密钥。激活方法文件 500 还包括列 520，其提供用于指示是否需要同时发送所有激活密钥或者是否一次仅发送激活密钥之一的信息。激活方法文件 500 还包括列 530，其标识要发送的参数，例如，完整的激活密钥、激活密钥类型编号、激活密钥的容量、用于计算激活密钥容量的值等等。

图 6 是根据本发明实施例的用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的方法的流程图 600。在图 6 中，确定激活密钥的参数和/或属性（610）。标识用于确认激活密钥的算法，并且创建激活密钥确认模板文件的 ASCII 版本（620）。提供用于将激活密钥确认模板文件的 ASCII 版本转换为二进制加密版本以及用于确认激活密钥的代码（630）。创建已知规则模板文件的 ASCII 版本，并将其转换为二进制加密已知规则模板文件（640）。

创建定制规则模板文件的 ASCII 版本，并将其转换为二进制加密定制规则模板文件（650）。提供激活方法文件的 ASCII 版本，并将其转换为二进制加密激活方法文件（660）。进行是否需要新的激活密钥类型的决策（670）。如果不需要（674），过程结束（698）。如果需要（672），则修改 ASCII 激活密钥确认模板文件，并将其转换为二进制加密激活密钥确认模板文件（680）。继而做出是否需要新的定制确认规则的决策（690）。如果不需要（692），过程结束（698）。如果需要（694），则修改定制规则模板文件的 ASCII 版本，并将其转换为二进制加密定制规则模板文件（696）。之后，过程结束（698）。

图 7 示出了根据本发明实施例的改变激活密钥确认模板文件 700 的示例。例如，如果需要在没有新的定制确认规则的情况下支持新的激活密钥类型 0x4 718，则针对激活密钥类型/编号为 0x4 718 的行更新激活密钥确认模板文件 700 的 ASCII 版本中的激活密钥描述。针对激活密钥类型/编号为 0x4 718 的行，在激活密钥确认模板文件 700 的 ASCII 版本中，将有效列 730 改变为“X”。针对激活密钥类型 0x4 718，将“X”放置在确认模板文件 700 的 ASCII 版本中的适当的确认规则列 740、770 中。对于这个具体示例，“X”被放置在密钥类型编号为 0x4 718 的行、确认规则 1 740 和确认规则 4 770 的列中。然后，可以执行用于将激活密钥确认模板文件的 ASCII 版本转换为二进制、加密版本的程序。

图 8 示出了根据本发明实施例的利用新的定制确认规则 880 来改变激活密钥确认模板文件 800 的示例。例如，如果需要利用新的定制确认规则 880 来支持新的激活密钥类型 0x4 818，则针对 0x4 818 激活密钥类型/编号的行更新激活密钥确认模板文件 800 的 ASCII 版本中的激活密钥描述。针对 0x4 818 激活密钥类型/编号的行，在激活密钥确认模板文件 800 的 ASCII 版本中，将有效列 830 更新为“X”。在激活密钥确认模板文件的 ASCII 版本中创建新的列，用于确认规则 5 880。针对激活密钥类型 0x4 818，将“X”846、874、882 放置在确认模板文件 800 的 ASCII 版本中的适当确认规则列中。对于这

个具体示例，“X”846、874、882被放置在密钥类型/编号0x4 818的行中、且分别在确认规则1 840、确认规则4 870和确认规则5 880的列中。执行用于将激活密钥确认模板文件800的ASCII版本转换为二进制加密版本的程序。

修改图4b所示的定制规则确认文件420的ASCII版本，使其具有用于确认规则5 440的行。图4b示出了被修改为具有确认规则5 440的描述“模型=123”442的定制规则确认文件420的ASCII版本。定制规则确认文件420的ASCII版本被修改为具有针对确认规则5 440的要检查项“模型”444。定制规则确认文件420的ASCII版本被修改为具有用于确认规则5 440的检查值“123”466。如果对于确认规则5 440的确认是良好的430，则将定制规则确认文件420的ASCII版本修改为使动作“确认通过”448运行。如果对于确认规则5 440的确认是不良的432，则将定制规则确认文件420的ASCII版本修改为使动作“显示确认错误—错的模型”450运行。最后，执行用于将定制规则确认文件420的ASCII版本转换为二进制加密版本的程序。

因此，本发明的实施例提供了用于改变和添加用于数字内容的功能的激活密钥而不必改变和重编译该数字内容的方法和装置。使用二进制加密模板文件确认激活密钥类型。二进制加密模板文件防止未授权的用户访问和改变确认模板文件。还使用二进制加密规则模板文件指明检查的功能使得当需要添加新的检查方法时不必写代码。提供二进制加密激活方法文件以指示代码如何对激活密钥进行激活。

本发明的示范实施例的上述描述是为举例描述而给出的。不是要穷举或将本发明限制为所公开的精确形式。在以上精神的启发下，很多修改和变更是可能的。本发明的范围不是要限制于此详细描述，而是由此处所附的权利要求所限制。

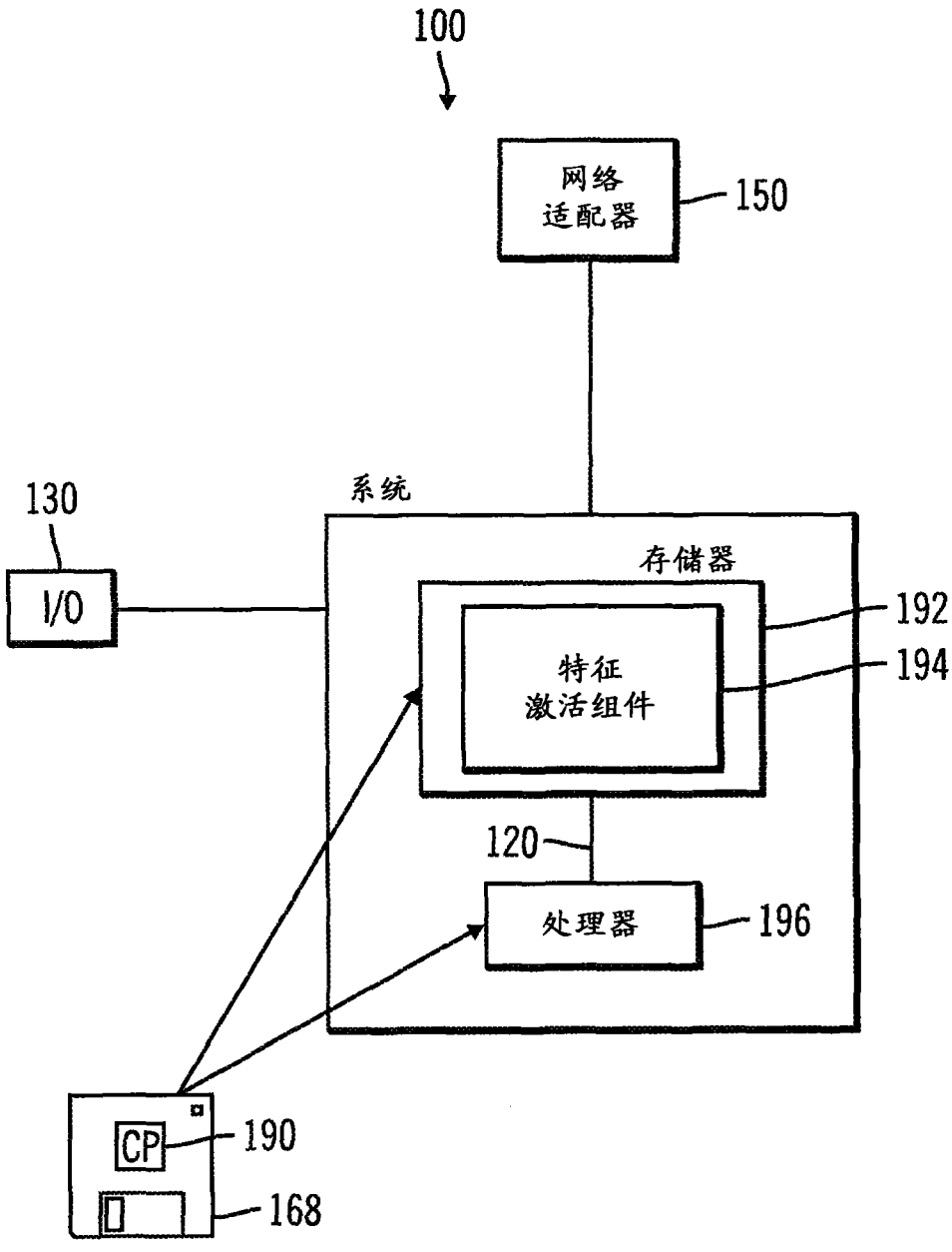

100
网络
适配器
150
130
I/O
系统
存储器
192
特征
激活组件
194
120
处理器
196
CP
190
168

图 1

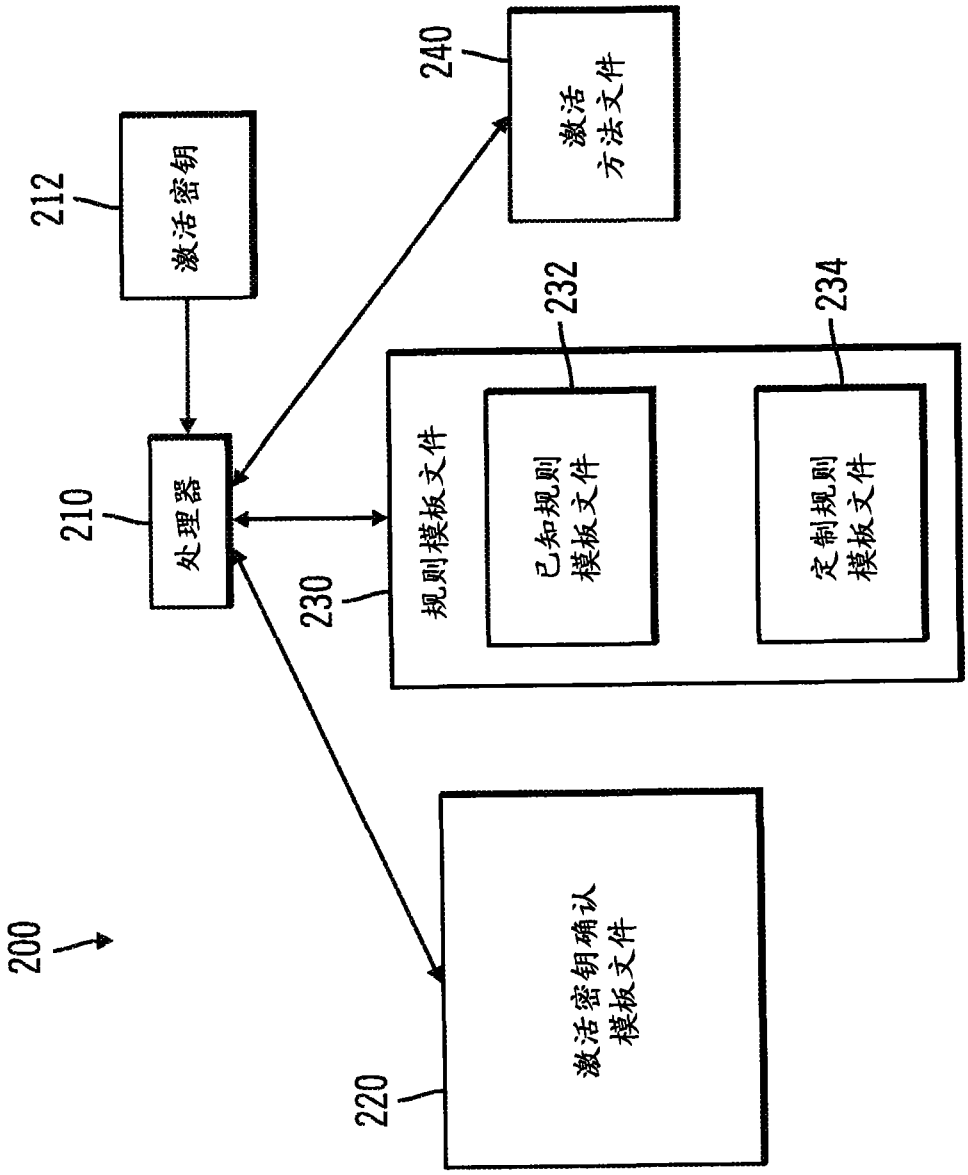

200
210
处理器
212
激活密钥
220
激活密钥确认
模板文件
230
规则模板文件
232
已知规则
模板文件
234
定制规则
模板文件
240
激活
方法文件

图 2

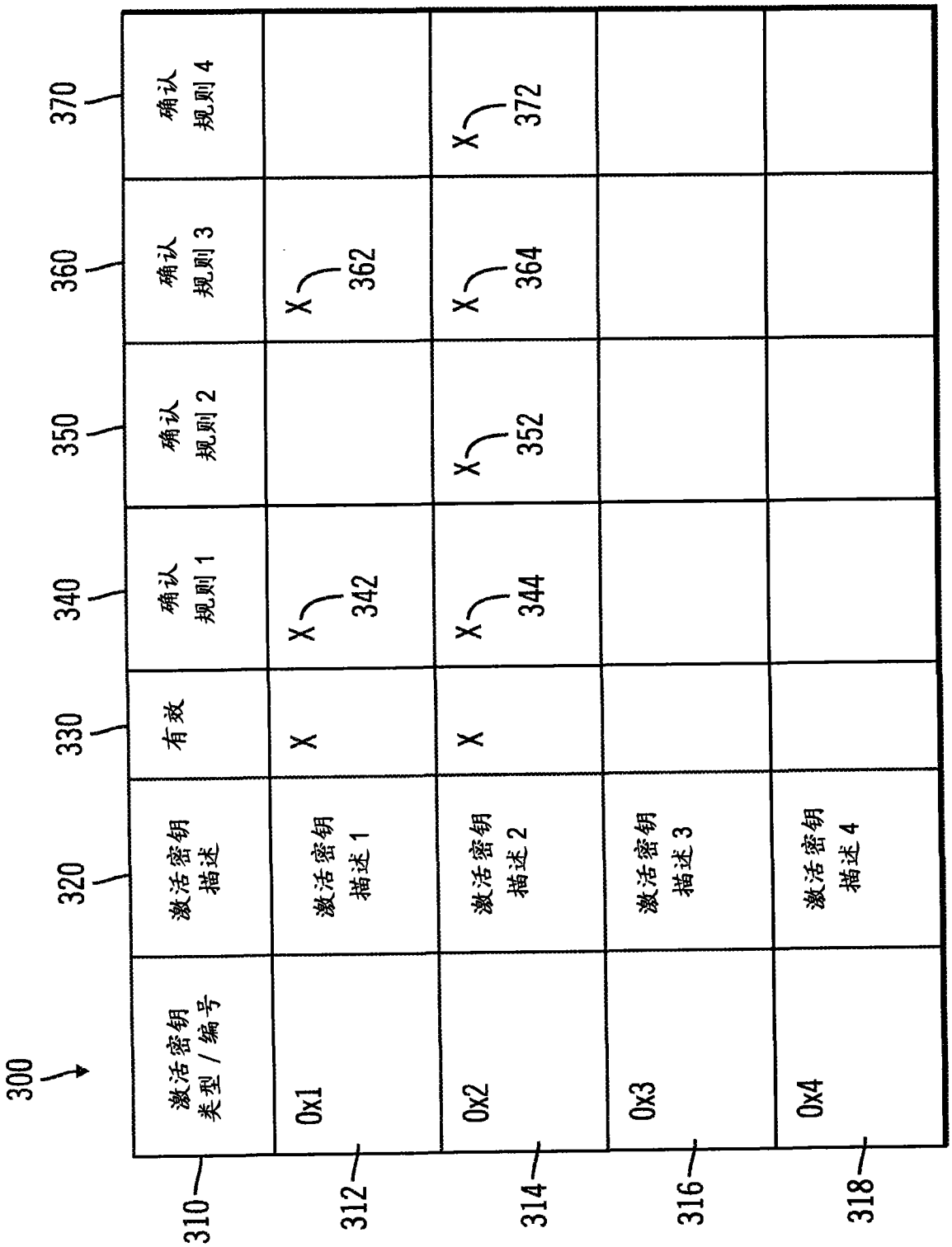

300
310
320
330
340
350
360
370
312
314
316
318
激活密钥类型/编号
激活密钥描述
有效
确认规则1
确认规则2
确认规则3
确认规则4
0x1
激活密钥描述1
X
X
342
362
0x2
激活密钥描述2
X
X
344
X
352
X
364
X
372
0x3
激活密钥描述3
0x4
激活密钥描述4

图 3

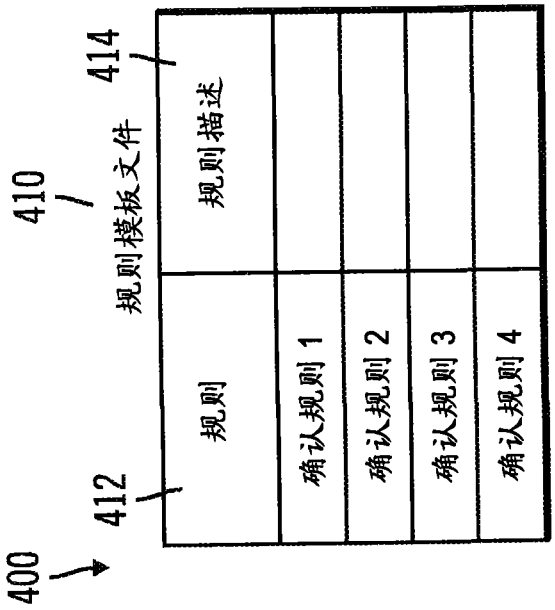

400
410
412
414
规则模板文件
规则
规则描述
确认规则 1
确认规则 2
确认规则 3
确认规则 4

图 4A

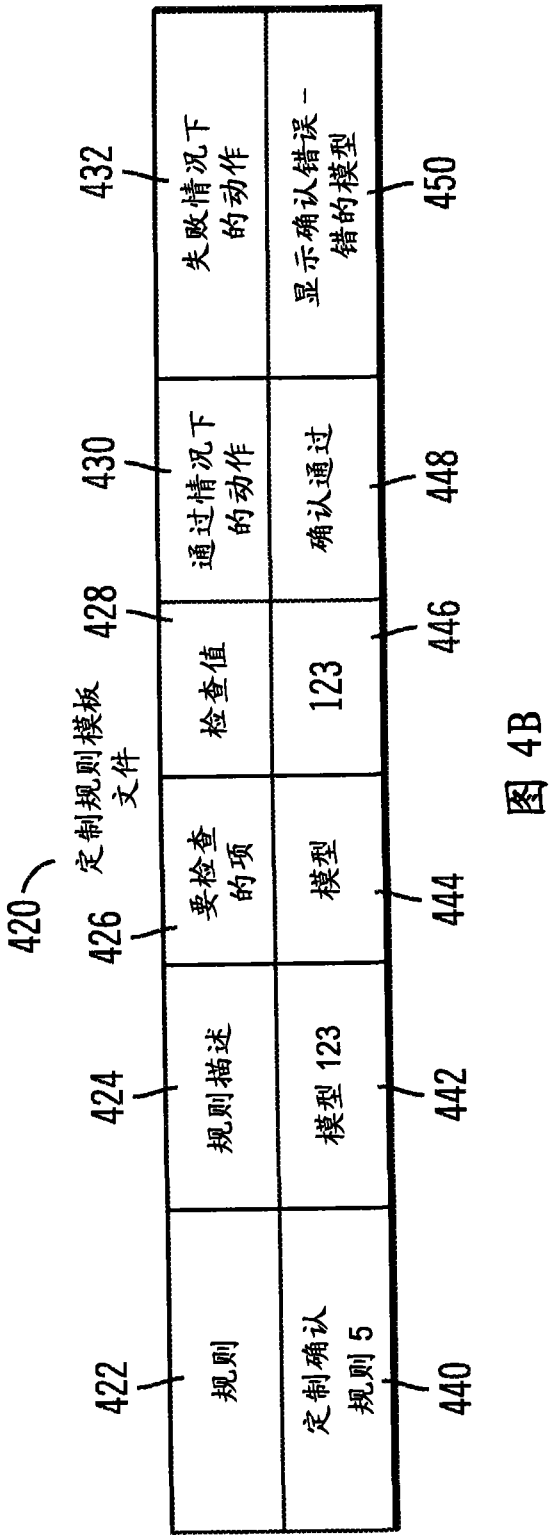

420
422
424
426
428
430
432
440
442
444
446
448
450
定制规则模板文件
规则
规则描述
要检查的项
检查值
通过情况下的动作
失败情况下的动作
定制确认规则 5
模型 123
模型
123
确认通过
显示确认错误 - 错的模型

图 4B

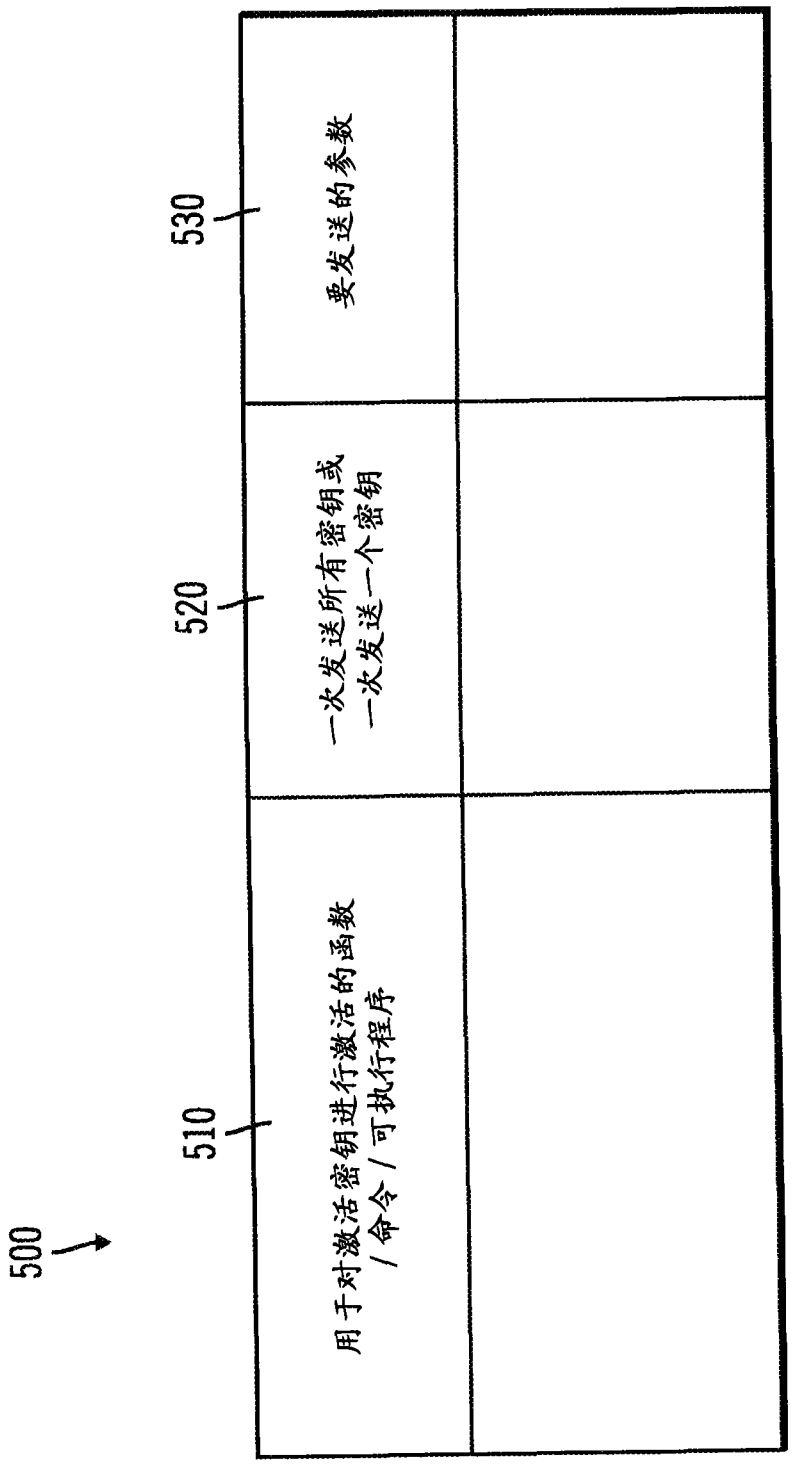

500
510
用于对激活密钥进行激活的函数
/命令/可执行程序
520
一次发送所有密钥或
一次发送一个密钥
530
要发送的参数

图 5

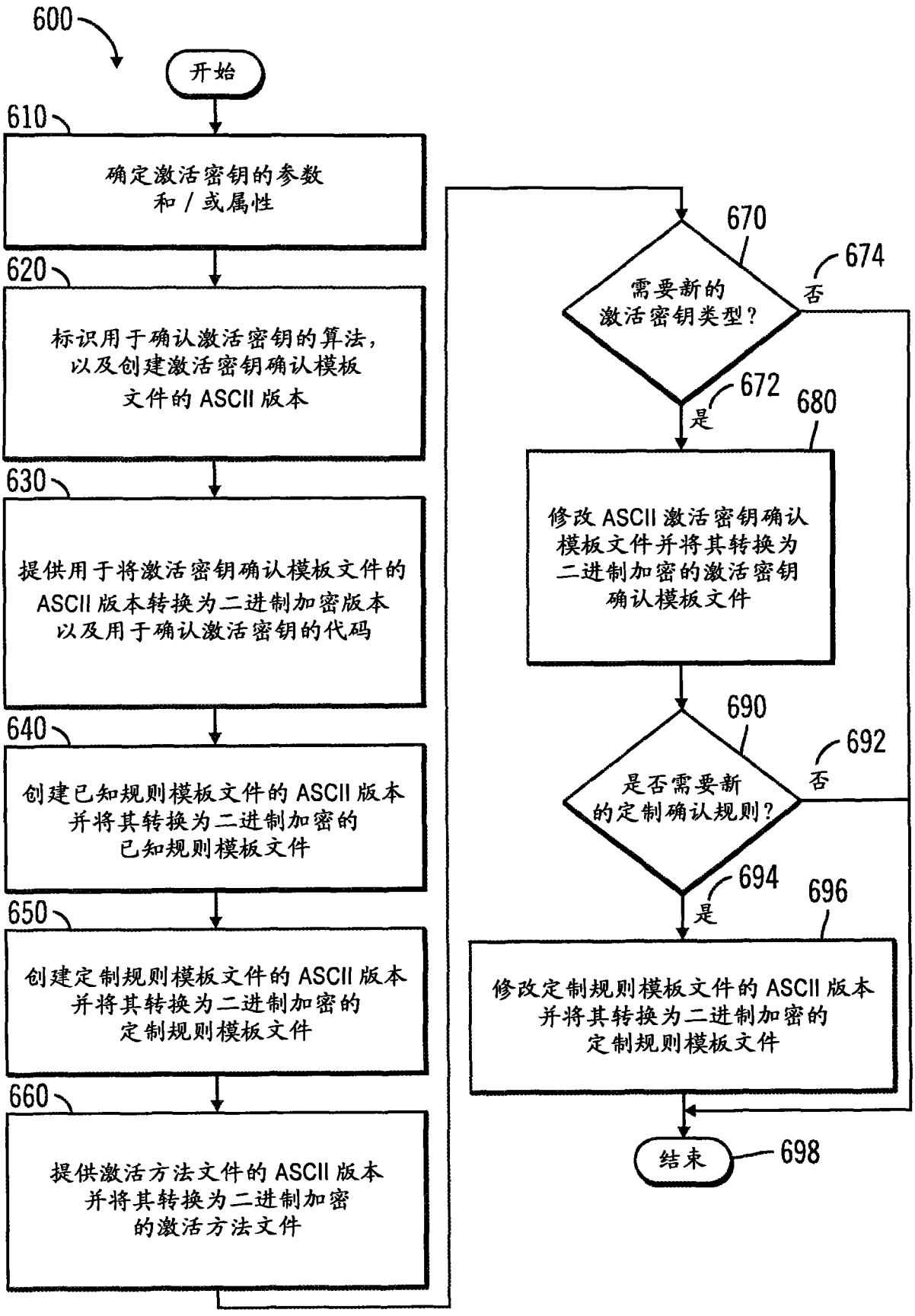

600
开始
610
确定激活密钥的参数
和 / 或属性
620
标识用于确认激活密钥的算法，
以及创建激活密钥确认模板
文件的 ASCII 版本
630
提供用于将激活密钥确认模板文件的
ASCII 版本转换为二进制加密版本
以及用于确认激活密钥的代码
640
创建已知规则模板文件的 ASCII 版本
并将其转换为二进制加密的
已知规则模板文件
650
创建定制规则模板文件的 ASCII 版本
并将其转换为二进制加密的
定制规则模板文件
660
提供激活方法文件的 ASCII 版本
并将其转换为二进制加密
的激活方法文件
670
需要新的
激活密钥类型？
674
否
672
是
680
修改 ASCII 激活密钥确认
模板文件并将其转换为
二进制加密的激活密钥
确认模板文件
690
是否需要新
的定制确认规则？
692
否
694
是
696
修改定制规则模板文件的 ASCII 版本
并将其转换为二进制加密的
定制规则模板文件
结束
698

图 6

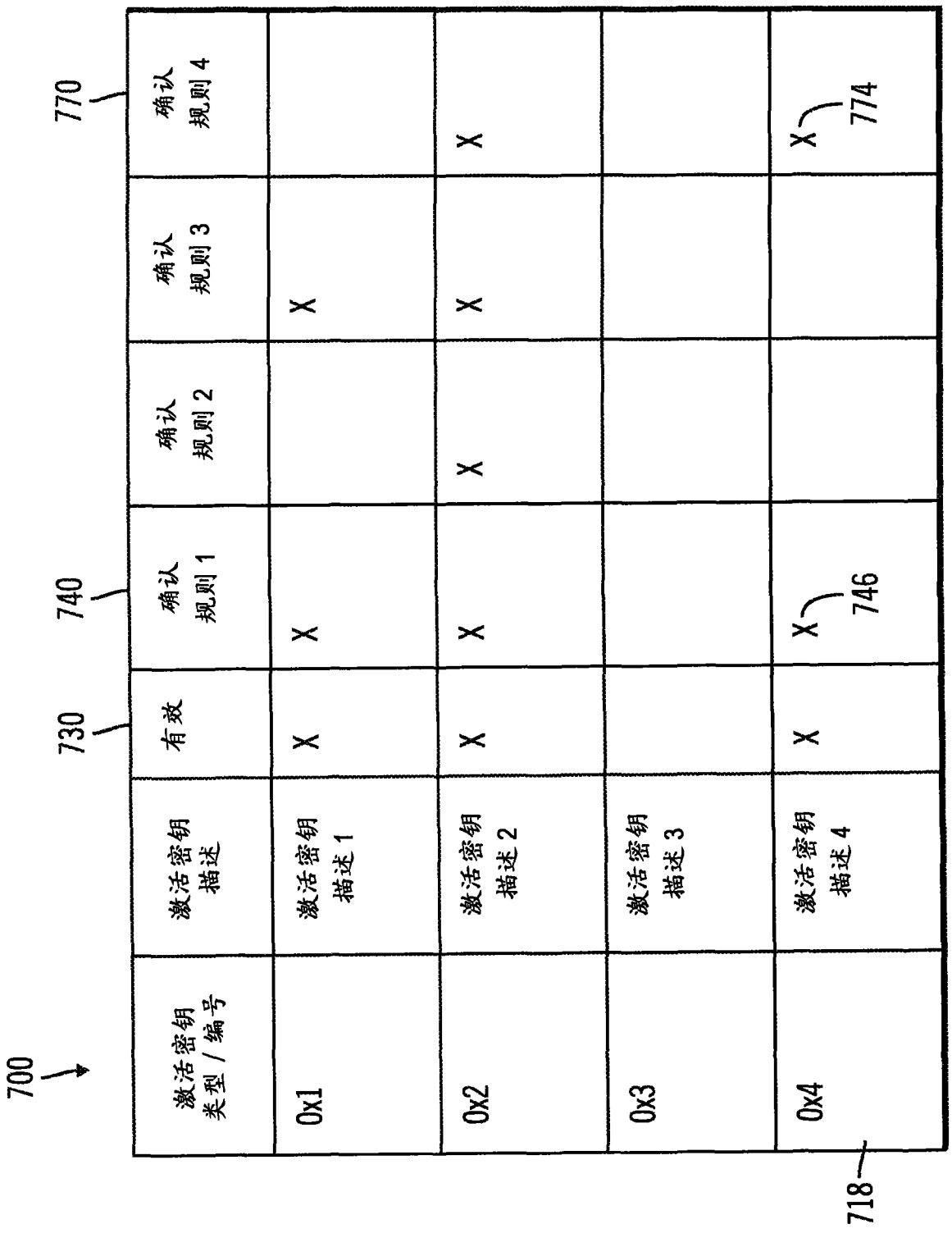

700
730
740
770
718
746
774
激活密钥类型 / 编号
激活密钥描述
有效
确认规则 1
确认规则 2
确认规则 3
确认规则 4
0x1
激活密钥描述 1
0x2
激活密钥描述 2
0x3
激活密钥描述 3
0x4
激活密钥描述 4
X

图 7

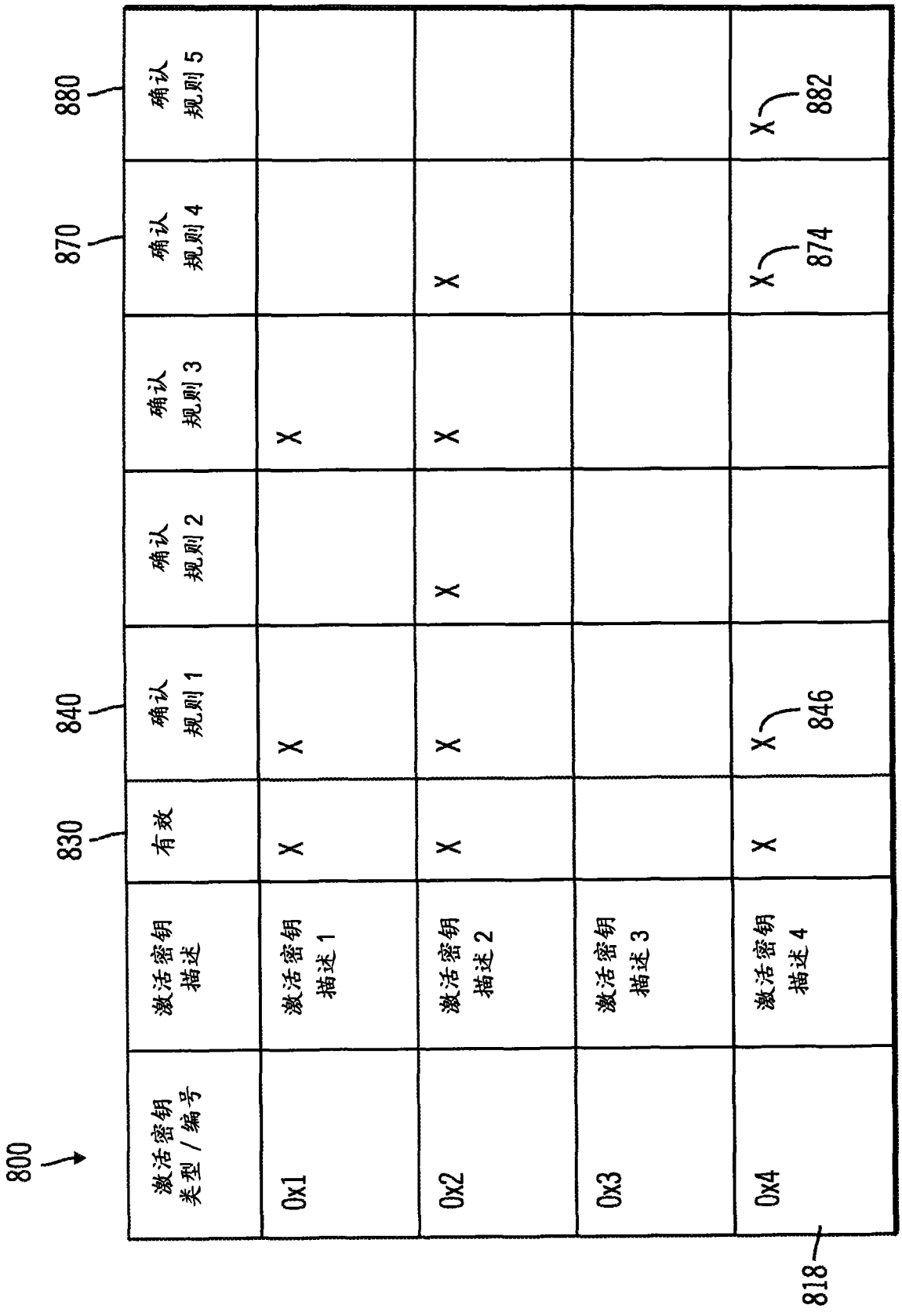

800
818
830
840
870
880
882
874
846
激活密钥类型 / 编号
激活密钥描述
有效
确认规则 1
确认规则 2
确认规则 3
确认规则 4
确认规则 5
0x1
激活密钥描述 1
X
X
0x2
激活密钥描述 2
X
X
X
X
0x3
激活密钥描述 3
0x4
激活密钥描述 4
X
X
X
X

图 8