电子设备及其密码验证方法

技术领域

本发明涉及信息安全技术领域，特别涉及一种用于电子设备的密码验证方法和电子设备。

背景技术

在使用例如 USBkey、智能卡等带有运算和数据存储改写功能的电子设备时，需要输入密码以开启 USBkey 或者智能卡。

现有的 USBkey 或者智能卡对于密码的校验都是逐位且等时地校验的，即对输入的字符串逐位地与正确密码进行比对，一旦出现错误位则返回错误提示。例如：假设正确密码为 123456，且校验每位密码所需的时间为 0.1ms，那么当输入密码“120000”时，USBkey 或者智能卡将在 0.3ms 返回密码错误提示；当输入密码“123000”时，USBkey 或者智能卡将在 0.4ms 返回密码错误提示。

现有技术存在的问题是，利用上述的反馈时间规律，不法分子可以根据密码提示信息的反馈时间推断出前几位密码的正确性，经过多次计算后即可窃取到完整的正确密码，造成电子设备密码的泄露，而电子设备密码一旦被获知，则导致了用户账号的不安全。

发明内容

本发明的目的旨在至少解决上述技术缺陷之一。

为达到上述目的，本发明第一个目的在于提出一种用于电子设备的密码验证方法，包括以下步骤：电子设备接收长度为 n 位字符串的输入密码，所述 n≥1；所述电子设备将所述输入密码的每个字符与预存的正确密码进行逐位比对或随机比对；所述电子设备在预定反馈时间或随机反馈时间返回比对结果，其中，所述预定反馈时间或所述随机反馈时间均不小于比对所述输入密码的 n 位字符串所需的时间。

根据本发明实施例的用于电子设备的密码验证方法，不管比对结果如何，电子设备均在预先设定的反馈时间或随机选择的反馈时间返回密码验证的结果，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

为达到上述目的，本发明第二个目的在于提出一种用于电子设备的密码验证方法，包

括以下步骤：电子设备接收长度为 n 位字符串的输入密码，所述 n≥1；所述电子设备对所述输入密码的每个字符与预存的正确密码进行随机比对；所述电子设备首次比对出所述字符与预存的正确密码不一致时，返回输入密码错误结果。

根据本发明实施例的用于电子设备的密码验证方法，电子设备对接收到的密码字符串中的每个字符不按顺序进行随机比对，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

为达到上述目的，本发明第三个目的在于提出一种电子设备，包括：接收模块，用于接收长度为 n 位字符串的输入密码，所述 n≥1；验证模块，用于将所述输入密码的每个字符与预存的正确密码进行逐位比对或随机比对；控制模块，用于在所述验证模块比对出结果后，在预定反馈时间或随机反馈时间输出所述比对结果，其中所述预定反馈时间或所述随机反馈时间均不小于比对所述输入密码的 n 位字符串所需的时间。

根据本发明实施例的电子设备，不管比对结果如何，电子设备均在预先设定的反馈时间或随机选择的反馈时间返回密码验证的结果，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

为达到上述目的，本发明第四个目的在于提出一种电子设备，包括：接收模块，用于接收长度为 n 位字符串的输入密码，所述 n≥1；验证模块，用于对所述输入密码的每个字符与预存的正确密码进行随机比对；控制模块，用于在首次比对出所述字符与预存的正确密码不一致时，输出输入密码错误结果。

根据本发明实施例的电子设备，电子设备对接收到的密码字符串中的每个字符不按顺序进行随机比对，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 为根据本发明实施例 1 的用于电子设备的密码验证方法的流程图；

图 2 为根据本发明实施例 2 的用于电子设备的密码验证方法的流程图；

图 3 为根据本发明实施例 3 的用于电子设备的密码验证方法的流程图；

图 4 为根据本发明实施例 4 的用于电子设备的密码验证方法的流程图；

图 5 为根据本发明实施例 5 的用于电子设备的密码验证方法的流程图；

图 6 为根据本发明实施例 6 的电子设备的结构框图。

具体实施方式

下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。相反，本发明的实施例包括落入所附加权利要求书的精神和内涵范围内的所有变化、修改和等同物。

在本发明的描述中，需要理解的是，术语 “第一”、“第二”等仅用于描述目的，而不能理解为指示或暗示相对重要性。在本发明的描述中，需要说明的是，除非另有明确的规定和限定，术语 “相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。此外，在本发明的描述中，除非另有说明，“多个”的含义是两个或两个以上。

流程图中或在此以其他方式描述的任何过程或方法描述可以被理解为，表示包括一个或更多个用于实现特定逻辑功能或过程的步骤的可执行指令的代码的模块、片段或部分，并且本发明的优选实施方式的范围包括另外的实现，其中可以不按所示出或讨论的顺序，包括根据所涉及的功能按基本同时的方式或按相反的顺序，来执行功能，这应被本发明的实施例所属技术领域的技术人员所理解。

下面参考附图描述根据本发明实施例的用于电子设备的密码验证方法。

实施例 1

图 1 为根据本发明实施例 1 的用于电子设备的密码验证方法的流程图。

根据本发明实施例 1 的用于电子设备的密码验证方法，不管比对结果如何都在预定反馈时间返回密码验证结果。

如图 1 所示，根据本发明实施例的用于电子设备的密码验证方法包括下述步骤。

步骤 S101，电子设备接收长度为 n 位字符串的输入密码，其中，n≥1。

例如，用户可以通过电子设备上的按键输入长度为 n 位的字符串密码；或者可以通过无线通信等方式接收输入密码。

步骤 S102，电子设备将输入密码的每个字符与预存的正确密码进行逐位比对。

步骤 S103，电子设备在预定反馈时间返回比对结果，其中，预定反馈时间不小于比对输入密码的 n 位字符串所需的时间。

例如，假设正确密码为 6 位密码 123456，且校验密码的每个字符所需的时间为 0.1ms，那么逐位比对该密码全部字符所需的时间为 0.6ms，因此用户可设置预定反馈时间为不小于 0.6ms，从而保证能够正确地完成密码验证。例如，可设定预定反馈时间为 0.6ms，不论比对结果如何，电子设备均在 0.6ms 反馈结果。应理解，预定反馈时间的设置不宜过大，以免浪费用户的时间，降低效率。

此外，对于反馈时间的控制，可以采用延时处理，也可以采用冗余计算的方式。例如，在电子设备中设置延时器，密码验证输出的结果信号均输入延时器，通过延时器控制其在预定反馈时间进行输出。

根据本发明实施例的用于电子设备的密码验证方法，不管比对结果如何，电子设备均在预先设定的反馈时间后返回密码验证的结果，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

实施例 2

图 2 为根据本发明实施例 2 的用于电子设备的密码验证方法的流程图。

实施例 2 的用于电子设备的密码验证方法与实施例 1 的方法相似，唯一的区别是，实施例 2 的用于电子设备的密码验证方法不管比对结果如何都在经过随机的时间后返回密码验证结果，而不是在固定的反馈时间后返回密码验证结果。

如图 2 所示，根据本发明实施例的用于电子设备的密码验证方法包括下述步骤。

步骤 S201，电子设备接收长度为 n 位字符串的输入密码，其中，n≥1。

步骤 S202，电子设备将输入密码的每个字符与预存的正确密码进行逐位比对。

步骤 S203，电子设备在随机反馈时间返回比对结果，其中，随机反馈时间不小于比对输入密码的 n 位字符串所需的时间。

当然，本实施例中，随机反馈时间还应该不大于预设时间，以免浪费用户的时间，降低效率。

例如，假设正确的密码为 6 位密码 123456，逐位校验密码的每个字符所需的时间为 0.1ms，校验完全部字符所需的时间为 0.6ms，并假设预设时间为 1ms，那么当输入的校验密码为“123000”时，生成的随机反馈时间可以为[0.6ms，1ms]区间内的任意值，由此保

证正确地完成密码验证，同时限定用户等待结果的预设时间，提高效率。

此外，对于反馈时间的控制，可以在预设时间范围内任意随机选择反馈时间，以便在所选择的反馈时间返回比对结果。

根据本发明实施例的用于电子设备的密码验证方法，不管比对结果如何，电子设备均在随机选择的时间返回密码验证的结果，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

实施例 3

图 3 为根据本发明实施例 3 的用于电子设备的密码验证方法的流程图。

根据本发明实施例 3 的用于电子设备的密码验证方法，电子设备对接收到的密码字符串进行不按顺序的随机比对。

如图 3 所示，根据本发明实施例的用于电子设备的密码验证方法包括下述步骤。

步骤 S301，电子设备接收长度为 n 位字符串的输入密码，其中，n≥1。

步骤 S302，电子设备将输入密码的每个字符与预存的正确密码进行随机比对。

步骤 S303，电子设备在预定反馈时间返回比对结果，其中，预定反馈时间不小于比对输入密码的 n 位字符串所需的时间。

假设正确密码为 6 位密码 123456，且校验密码的每个字符所需的时间为 0.1ms，那么随机比对该密码全部字符所需的时间为 0.6ms，因此用户可设置预定反馈时间为不小于 0.6ms，从而保证能够正确地完成密码验证，同时对该 6 位密码进行随机选择字符比对，例如，首先比对第 4 位，再比对第 1 位等，比对位可以任意随机选择。例如：设定预定反馈时间为 0.6ms，此时，不论比对结果如何，电子设备均在 0.6ms 反馈结果。应理解，预定反馈时间的设置不宜过大，以免浪费用户的时间，降低效率。

根据本发明实施例的用于电子设备的密码验证方法，不管比对结果如何，电子设备均在预先设定的反馈时间后返回密码验证的结果，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

实施例 4

实施例 4 的用于电子设备的密码验证方法与实施例 3 的方法相似，唯一的区别是，实施例 4 的用于电子设备的密码验证方法不管比对结果如何都在经过随机的时间后返回密码验证结果，而不是在固定的反馈时间后返回密码验证结果。

如图 4 所示，根据本发明实施例的用于电子设备的密码验证方法包括下述步骤。

步骤 S401，电子设备接收长度为 n 位字符串的输入密码，其中，n≥1。

步骤 S402，电子设备将输入密码的每个字符与预存的正确密码进行随机比对。

步骤 S403，电子设备在随机反馈时间返回比对结果，其中，随机反馈时间不小于比对输入密码的 n 位字符串所需的时间。

例如，假设正确的密码为 6 位密码 123456，随机校验密码的每个字符所需的时间为 0.1ms，校验完全部字符所需的时间为 0.6ms，并假设预设时间为 1ms，那么当输入的校验密码为“123000”时，生成的随机反馈时间可以为[0.6ms，1ms]区间内的任意值，由此保证正确地完成密码验证，同时限定用户等待结果的预设时间，提高效率。

根据本发明实施例的用于电子设备的密码验证方法，不管比对结果如何，电子设备均在随机选择的时间返回密码验证的结果，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

实施例 5

图 5 为根据本发明实施例 5 的用于电子设备的密码验证方法的流程图。

根据本发明实施例 5 的用于电子设备的密码验证方法，电子设备对接收到的密码字符串进行不按顺序的随机比对。

如图 5 所示，根据本发明实施例的用于电子设备的密码验证方法包括下述步骤。

步骤 S501，电子设备接收长度为 n 位字符串的输入密码，其中，n≥1

步骤 S502，电子设备对输入密码的每个字符与预存的正确密码进行随机比对。

步骤 S503，电子设备首次比对出字符与预存的正确密码不一致时，返回输入密码错误结果。

例如，假设正确密码是 6 位密码“123456”，且校验密码的每个字符所需的时间为 0.1ms，那么当校验密码字符串是“123000”，且首先比对第 4 位时，在 0.1ms 就会输出密码错误的提示。由此，如果不法分子意欲破解密码，将会认为第 1 位是错误的而更改第 1 位字符后重新输入，而事实是第 1 位字符是正确的，因此避免了不法分子根据反馈时间的规律破解密码的可能性，提高了密码的安全性。

根据本发明实施例的用于电子设备的密码验证方法，电子设备对接收到的密码字符串不按顺序进行随机比对，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

下面参考附图详细描述根据本发明实施例的电子设备。

实施例 6

图 6 为本发明实施例 6 的电子设备的结构框图。

如图 6 所示，根据本发明实施例的电子设备包括接收模块 110、验证模块 120、控制模块 130。具体的：

接收模块 110 用于接收长度为 n 位字符串的输入密码，其中，n≥1；

验证模块 120 用于将输入密码的每个字符与预存的正确密码进行逐位比对或随机比对；

控制模块 130 用于在验证模块比对出结果后，在预定反馈时间或随机反馈时间输出比对结果，其中预定反馈时间或随机反馈时间均不小于比对输入密码的 n 位字符串所需的时间。或者

控制模块 130 用于在验证模块 120 对输入密码的每个字符与预存的正确密码进行随机比对时，首次比对出字符与预存的正确密码不一致时，输出输入密码错误结果。

此外，该电子设备还可以包括：显示模块 140；

显示模块 140 用于接收控制模块输出的比对结果，并对比对结果进行显示；或者

显示模块 140 用于接收控制模块输出的输入密码错误结果，并对输入密码错误结果进行显示。

进一步的，控制模块 130 可以通过延时处理的方式或冗余计算的方式控制在预定反馈时间输出比对结果。控制模块 130 还可以随机选择反馈时间，控制在所选择的反馈时间输出比对结果。

当然，预定反馈时间的设置不宜过大，以免浪费用户的时间，降低效率；随机反馈时间不宜大于预设时间，以免浪费用户的时间，降低效率。

当然，本实施例中电子设备可以为电子签名工具或智能卡。

根据本发明实施例的电子设备，不管比对结果如何，电子设备均在预先设定的反馈时间或随机选择的反馈时间返回密码验证的结果，或者电子设备对接收到的密码字符串中的每个字符不按顺序进行随机比对，由此网络上的不法分子无法根据反馈时间规律计算出完整的正确密码，提高了电子设备的密码的安全性，从而提高了用户账号的安全性。

尽管已经示出和描述了本发明的实施例，对于本领域的普通技术人员而言，可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行多种变化、修改、替换和变型，本发明的范围由所附权利要求及其等同限定。

权利要求书

1、一种用于电子设备的密码验证方法，其特征在于，该方法包括以下步骤：

电子设备接收长度为 n 位字符串的输入密码，所述 n≥1；

所述电子设备将所述输入密码的每个字符与预存的正确密码进行逐位比对或随机比对；

所述电子设备在预定反馈时间或随机反馈时间返回比对结果，其中，所述预定反馈时间或所述随机反馈时间均不小于比对所述输入密码的 n 位字符串所需的时间。

2、根据权利要求 1 所述的方法，其特征在于，所述电子设备在预定反馈时间返回比对结果包括：

通过延时处理控制所述电子设备在所述预定反馈时间返回比对结果；

或者，采用冗余计算的方式控制所述电子设备在所述预定反馈时间返回比对结果。

3、根据权利要求 1 所述的方法，其特征在于，所述电子设备在随机反馈时间返回比对结果包括：

随机选择反馈时间，控制所述电子设备在所选择的反馈时间返回比对结果。

4、根据权利要求 1 或 3 所述的方法，其特征在于，所述随机反馈时间不大于预设时间。

5、根据权利要求 1-3 任一项所述的方法，其特征在于，所述电子设备为电子签名工具或智能卡。

6、一种用于电子设备的密码验证方法，其特征在于，该方法包括以下步骤：

电子设备接收长度为 n 位字符串的输入密码，所述 n≥1；

所述电子设备对所述输入密码的每个字符与预存的正确密码进行随机比对；

所述电子设备首次比对出所述字符与预存的正确密码不一致时，返回输入密码错误结果。

7、一种电子设备，其特征在于，该电子设备包括：

接收模块，用于接收长度为 n 位字符串的输入密码，所述 n≥1；

验证模块，用于将所述输入密码的每个字符与预存的正确密码进行逐位比对或随机比对；

控制模块，用于在所述验证模块比对出结果后，在预定反馈时间或随机反馈时间输出所述比对结果，其中所述预定反馈时间或所述随机反馈时间均不小于比对所述输入密码的 n 位字符串所需的时间。

8、根据权利要求 7 所述的电子设备，其特征在于，所述控制模块通过延时处理的方式或冗余计算的方式控制在所述预定反馈时间输出比对结果。

9、根据权利要求 7 所述的电子设备，其特征在于，所述控制模块随机选择反馈时间，控制在所选择的反馈时间输出比对结果。

10、根据权利要求 7 或 9 所述的电子设备，其特征在于，所述随机反馈时间不大于预设时间。

11、根据权利要求 7-9 任一项所述的电子设备，其特征在于，该电子设备还包括：显示模块；

所述显示模块用于接收所述控制模块输出的比对结果，并对所述比对结果进行显示。

12、根据权利要求 7-9 任一项所述电子设备， 其特征在于，所述电子设备为电子签名工具或智能卡。

13、一种电子设备，其特征在于，该电子设备包括：

接收模块，用于接收长度为 n 位字符串的输入密码，所述 n≥1；

验证模块，用于对所述输入密码的每个字符与预存的正确密码进行随机比对；

控制模块，用于在首次比对出所述字符与预存的正确密码不一致时，输出输入密码错误结果。

14、根据权利要求 13 所述的电子设备，其特征在于，该电子设备还包括：显示模块；

所述显示模块用于接收所述控制模块输出的输入密码错误结果，并对所述输入密码错误结果进行显示。

15、根据权利要求 13 或 14 所述电子设备，其特征在于，所述电子设备为电子签名工具或智能卡。