(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119856446 A
(43)申请公布日 2025.04.18

(21)申请号 202280099418.5
(22)申请日 2022.08.31
(85)PCT国际申请进入国家阶段日
2025.02.21
(86)PCT国际申请的申请数据
PCT/JP2022/032875 2022.08.31
(87)PCT国际申请的公布数据
WO2024/047821 JA 2024.03.07
(71)申请人 本田技研工业株式会社
地址 日本东京
(72)发明人 原田裕考
(74)专利代理机构 北京鸿德海业知识产权代理有限公司 11412
专利代理师 柳海林
(51)Int.Cl.
H04L 9/32(2006.01)
G06F 21/44(2006.01)

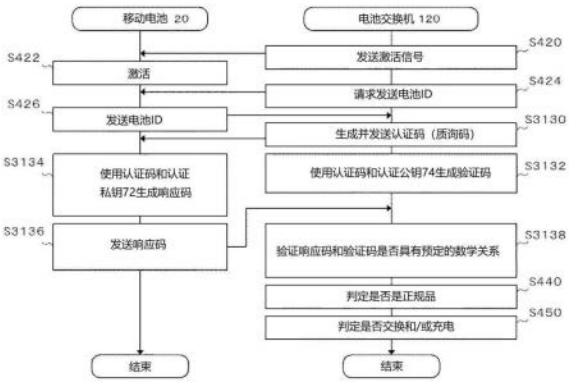
权利要求书5页 说明书39页 附图8页

(54)发明名称

确认方法、确认装置、蓄电装置、确认系统、程序以及计算机可读存储介质

(57)摘要

本发明提供一种确认方法。上述确认方法具有:将第一验证信息向待确认装置发送的步骤;基于第二验证信息对第一验证信息进行变换并生成第三验证信息的步骤;从待确认装置接收第五验证信息或第六验证信息的步骤,其中,(i)第五验证信息是待确认装置基于和第二验证信息满足第一数学关系的第四验证信息对第一验证信息进行变换而生成的信息,(ii)第六验证信息是待确认装置使用在待确认装置是合法装置时第三验证信息以及第五验证信息应该满足的第二数学关系而根据第一验证信息以及第四验证信息导出的或根据第五验证信息导出的信息;基于第三验证信息、以及第五验证信息或第六验证信息,判定待确认装置是否是合法装置的步骤。



CN 119856446 A

1.一种确认方法,是确认装置用于确认待确认装置是否是合法装置的确认方法,具有:

将第一验证信息向所述待确认装置发送的步骤;

通过基于第二验证信息对所述第一验证信息进行变换而生成第三验证信息的步骤;

从所述待确认装置接收第五验证信息或第六验证信息的步骤,其中,(i)所述第五验证信息是所述待确认装置基于和所述第二验证信息满足第一数学关系的第四验证信息对所述第一验证信息进行变换而生成的信息,(i i)所述第六验证信息是所述待确认装置使用在待确认装置是合法装置时所述第三验证信息以及所述第五验证信息应该满足的第二数学关系而根据所述第一验证信息以及所述第四验证信息导出的或根据所述第五验证信息导出的信息;以及

基于所述第三验证信息、以及所述第五验证信息或所述第六验证信息,判定所述待确认装置是否是合法装置的步骤,

所述进行判定的步骤包含:

(a)在所述第五验证信息被接收到时,判定所述第三验证信息以及所述第五验证信息是否满足所述第二数学关系的步骤,或者,

(b)在所述第六验证信息被接收到时,判定所述第三验证信息以及所述第六验证信息是否一致的步骤,

所述第二数学关系基于所述第一数学关系来确定。

2.根据权利要求1所述的确认方法,其中,

判定所述第三验证信息以及所述第五验证信息是否满足所述第二数学关系的步骤包含:

按照第一验证算法对所述第三验证信息以及所述第五验证信息进行信息处理来生成第七验证信息的步骤;

从所述待确认装置获取第八验证信息的步骤,所述第八验证信息表示在所述第二验证信息以及所述第四验证信息满足所述第一数学关系时,按照所述第一验证算法对所述第三验证信息以及所述第五验证信息进行信息处理而会得到的运算结果;以及

判定所述第七验证信息以及所述第八验证信息是否一致的步骤。

3.根据权利要求1或2所述的确认方法,其中,

还具有:在判定为所述第三验证信息以及所述第五验证信息不满足所述第二数学关系的情况下,或者在判定为所述第三验证信息以及所述第六验证信息不一致的情况下,确认为所述待确认装置不是合法装置,或者所述待确认装置是非合法装置的步骤。

4.根据权利要求1至3中任一项所述的确认方法,其中,

还具有:在判定为所述第三验证信息以及所述第五验证信息满足所述第二数学关系的情况下,或者在判定为所述第三验证信息以及所述第六验证信息一致的情况下,确认为所述待确认装置是合法装置,或者所述待确认装置不是非合法装置的步骤。

5.根据权利要求1至4中任一项所述的确认方法,其中,还具有:

(i)从所述确认装置的制造者或转让者、或者所述第二验证信息以及所述第四验证信息的发行者获取所述第二验证信息,或者(ii)从构成为能够与所述确认装置进行无线通信并且确认为所述确认装置是合法装置的第一外部装置获取所述第二验证信息的步骤;以及

将获取的所述第二验证信息保存至配置于所述确认装置的第一存储装置的步骤。

6.根据权利要求1至5中任一项所述的确认方法,其中,还具有:

(i)从所述待确认装置的制造者或转让者、或者所述第二验证信息以及所述第四验证信息的发行者获取所述第四验证信息,或者(i i)从构成为能够与所述待确认装置进行无线通信并且确认为所述待确认装置是合法装置的第二外部装置获取所述第四验证信息的步骤;以及

将获取的所述第四验证信息保存至配置于所述待确认装置的第二存储装置的步骤。

7.根据权利要求1至6中任一项所述的确认方法,其中,还具有:

从所述待确认装置接收被使用第一私钥加密的所述第二验证信息的步骤;以及

使用与所述第一私钥对应的第一公钥对所述加密的所述第二验证信息解密的步骤。

8.根据权利要求7所述的确认方法,其中,还具有:

从所述待确认装置接收未被加密的所述第二验证信息的步骤;以及

判定未被加密的所述第二验证信息和解密的所述第二验证信息是否一致的步骤,

生成所述第三验证信息的所述步骤包含:

在所述进行判定的步骤中判定为未被加密的所述第二验证信息以及解密的所述第二验证信息一致的情况下,基于所述第二验证信息对所述第一验证信息进行变换并生成所述第三验证信息的步骤。

9.根据权利要求1至6中任一项所述的确认方法,其中,还具有:

从所述待确认装置获取使用第一私钥签名的所述第二验证信息的步骤;以及

使用与所述第一私钥对应的第一公钥对所述签名进行验证的步骤。

10.根据权利要求9所述的确认方法,其中,

所述获取签名的所述第二验证信息的步骤包含:

获取使用所述第一私钥加密的所述第二验证信息和未被加密的所述第二验证信息的步骤,

所述对签名进行验证的步骤包含:

使用所述第一公钥对加密的所述第二验证信息进行解密的步骤;以及

判定未被加密的所述第二验证信息和解密的所述第二验证信息是否一致的步骤,

生成所述第三验证信息的所述步骤包含:

在所述进行判定的步骤中判定为未被加密的所述第二验证信息以及解密的所述第二验证信息一致的情况下,基于所述第二验证信息对所述第一验证信息进行变换并生成所述第三验证信息的步骤。

11.根据权利要求1至10中任一项所述的确认方法,其中,

所述第二验证信息是公钥,

所述第四验证信息是与所述公钥对应的私钥。

12.根据权利要求1至11中任一项所述的确认方法,其中,还具有:

生成随机数的步骤;以及

基于所述随机数来生成所述第一验证信息的步骤。

13.根据权利要求1至12中任一项所述的确认方法,其中,还具有:

所述待确认装置从所述确认装置接收所述第一验证信息的步骤;

所述待确认装置基于所述第一验证信息以及所述第四验证信息来生成所述第五验证

信息的步骤;以及

所述待确认装置将生成的所述第五验证信息向所述确认装置发送的步骤。

14.根据权利要求1至13中任一项所述的确认方法,其中,

所述待确认装置具备蓄电装置,

所述确认装置具备构成为能够相对于所述蓄电装置进行拆装,并且使所述蓄电装置进行充电以及/或放电的充放电装置。

15.根据权利要求1至14中任一项所述的确认方法,其中,

所述确认装置是具有第一端子的第一电力装置,

所述待确认装置是具有构成为能够与所述第一端子进行安装的第二端子的第二电力装置,

所述确认方法还具有:

在判定为所述第三验证信息以及所述第五验证信息不满足所述第二数学关系的情况下,或者在判定为所述第三验证信息以及所述第六验证信息不一致的情况下,决定禁止或者抑制所述第一电力装置以及所述第二电力装置之间的电力的输出输入的步骤。

16.根据权利要求1至15中任一项所述的确认方法,其中,

所述确认装置是将所述待确认装置作为待保管装置进行保管的保管装置,

所述保管装置具有供所述待保管装置安装的安装部,

所述确认方法还具有:

(a)在判定为所述第三验证信息以及所述第五验证信息不满足所述第二数学关系的情况下,或者在判定为所述第三验证信息以及所述第六验证信息不一致的情况下,决定不继续所述待保管装置相对于所述安装部的安装、或者以与合法装置不同的方式对所述待保管装置进行保管的步骤,以及/或者

(b)在判定为所述第三验证信息以及所述第五验证信息满足所述第二数学关系的情况下,或者在判定为所述第三验证信息以及所述第六验证信息一致的情况下,决定继续所述待保管装置相对于所述安装部的安装、或者将所述待保管装置作为合法装置进行保管的步骤。

17.根据权利要求16所述的确认方法,其中,

所述保管装置构成为能够对多个所述待保管装置的至少一个进行保管,

所述确认方法还具有:

获取用于识别多个所述待保管装置中的能够被多个利用者共同利用的所述待保管装置的共同利用识别信息的步骤;

在判定为所述第三验证信息以及所述第五验证信息满足所述第二数学关系的情况下,或者在判定为所述第三验证信息以及所述第六验证信息一致的情况下,基于所述共同利用识别信息,判定所述待确认装置是否是能够被多个所述利用者共同利用的所述待保管装置的步骤;以及

(c)在判定为所述待确认装置不是能够被多个所述利用者共同利用的所述待保管装置的情况下,决定不继续所述待保管装置相对于所述安装部的安装、或者以与合法装置不同的方式对所述待保管装置进行保管,以及/或者(d)在判定为所述待确认装置是能够被多个所述利用者共同利用的所述待保管装置的情况下,决定继续所述待保管装置相对于所述安

装部的安装、或者将所述待保管装置作为合法装置进行保管的步骤。

18.一种确认装置,是确认待确认装置是否是合法装置的确认装置,其中。具备:

第一验证信息发送部,其将第一验证信息发送至所述待确认装置;

第三验证信息生成部,其基于第二验证信息对所述第一验证信息进行变换而生成第三验证信息;

响应接收部,其从所述待确认装置接收第五验证信息或第六验证信息,其中,(i)所述第五验证信息是所述待确认装置基于和所述第二验证信息满足第一数学关系的第四验证信息对所述第一验证信息进行变换而生成的信息,(i i)所述第六验证信息是所述待确认装置使用在待确认装置是合法装置时所述第三验证信息以及所述第五验证信息应该满足的第二数学关系,根据所述第一验证信息以及所述第四验证信息导出的、或根据所述第五验证信息导出的信息;以及

判定部,其基于所述第三验证信息、以及所述第五验证信息或者所述第六验证信息,判定所述待确认装置是否是合法装置,

所述判定部进行如下处理:

(a)在接收到所述第五验证信息的情况下,判定所述第三验证信息以及所述第五验证信息是否满足所述第二数学关系,或者

(b)在接收到所述第六验证信息的情况下,判定所述第三验证信息以及所述第六验证信息是否一致。

19.一种蓄电装置,其具备:

蓄电部,其蓄积电能;

电端子,其用于与对所述蓄电部进行充电、或者利用所述蓄电部放电的电力的第一电力装置之间收发电力,

其中,所述蓄电装置还具备:

保存部,其保存第四验证信息;

第一验证信息获取部,其从所述第一电力装置获取第一验证信息;以及

响应部,其通过基于所述保存部所保存的所述第四验证信息对所述第一验证信息获取部所获取的所述第一验证信息进行变换而生成第五验证信息,或者基于和所述第四验证信息满足第一数学关系的第二验证信息,生成对所述第一验证信息进行变换而得到的第六验证信息。

20.根据权利要求19所述的蓄电装置,其中,

所述响应部将所述第五验证信息或者所述第六验证信息发送至所述第一电力装置。

21.一种确认系统,其中,具备:

电力装置,其具有权利要求18所述的确认装置;以及

权利要求19或者权利要求20所述的蓄电装置,

所述确认装置确认为作为所述确认装置的确认对象亦即待确认装置的所述蓄电装置是合法装置。

22.一种程序,其中,

所述程序用于使计算机执行权利要求1至17中任一项所述的确认方法。

23.一种计算机可读的存储介质,其中,

存储有权利要求22所述的程序。

确认方法、确认装置、蓄电装置、确认系统、程序以及计算机可读存储介质

技术领域

[0001] 本发明涉及确认方法、确认装置、蓄电装置、确认系统、程序以及计算机可读存储介质。

背景技术

[0002] 在专利文献1中,公开了通过对返还至电池站的电池中保存的认证密钥和电池站中保存的认证密钥进行核对,来认证电池的管理装置。在专利文献2中,公开了利用白名单方式,判断可否进行电池的受理的电池站。

[0003] 专利文献1:国际公开第2019/181661号

[0004] 专利文献2:国际公开第2020/059833号

发明内容

[0005] 在本发明的第一方式中,提供一种确认方法。上述确认方法例如是确认装置用于确认待确认装置是否是合法装置的确认方法。上述确认方法例如具有将第一验证信息向待确认装置发送的步骤。上述确认方法例如具有基于第二验证信息对第一验证信息进行变换而生成第三验证信息的步骤。上述确认方法例如具有从待确认装置接收第五验证信息或第六验证信息的步骤,其中,(i)第五验证信息是待确认装置基于和第二验证信息满足第一数学关系的第四验证信息对第一验证信息进行变换而生成的信息,(i i)第六验证信息是待确认装置使用在待确认装置是合法装置时第三验证信息以及第五验证信息应该满足的第二数学关系而根据第一验证信息以及第四验证信息导出的或根据第五验证信息导出的信息。上述确认方法例如具有基于第三验证信息、以及第五验证信息或第六验证信息,判定待确认装置是否是合法装置的步骤。在上述确认方法中,进行判定的步骤例如包含:(a)在接收到第五验证信息时,判定第三验证信息以及第五验证信息是否满足第二数学关系的步骤,或者,(b)在接收到第六验证信息时,判定第三验证信息以及第六验证信息是否一致的步骤。在上述确认方法中,第二数学关系基于第一数学关系来确定。

[0006] 在上述任一确认方法中,判定第三验证信息以及第五验证信息是否满足第二数学关系的步骤可以包含:按照第一验证算法对第三验证信息以及第五验证信息进行信息处理来生成第七验证信息的步骤。在上述任一确认方法中,上述判定的步骤可以包含从待确认装置获取第八验证信息的步骤,所述第八验证信息表示在第二验证信息以及第四验证信息满足第一数学关系时,按照第一验证算法对第三验证信息以及第五验证信息进行信息处理而会得到的运算结果。在上述任一确认方法中,上述判定的步骤可以包含判定第七验证信息以及第八验证信息是否一致的步骤。

[0007] 在上述任一确认方法中,还可以具有:在判定为第三验证信息以及第五验证信息不满足第二数学关系的情况下,或者在判定为第三验证信息以及第六验证信息不一致的情况下,确认为待确认装置不是合法装置,或者待确认装置是非合法装置的步骤。在上述任一

确认方法中,还可以具有:在判定为第三验证信息以及第五验证信息满足第二数学关系的情况下,或者在判定为第三验证信息以及第六验证信息一致的情况下,确认为待确认装置是合法装置,或者待确认装置不是非合法装置的步骤。

[0008] 在上述任一确认方法中,还可以具有:(i)从确认装置的制造者或转让者、或者第二验证信息以及第四验证信息的发行者获取第二验证信息,或者(i i)从构成为能够与确认装置进行无线通信并且确认为确认装置是合法装置的第一外部装置获取第二验证信息的步骤。在上述任一确认方法中,还可以具有将获取的第二验证信息保存至配置于确认装置的第一存储装置的步骤。在上述任一确认方法中,还可以具有:(i)从待确认装置的制造者或转让者、或者第二验证信息以及第四验证信息的发行者获取第四验证信息,或者(i i)从构成为能够与待确认装置进行无线通信并且确认为待确认装置是合法装置的第二外部装置获取第四验证信息的步骤。在上述任一确认方法中,还可以具有将获取的第四验证信息保存至配置于待确认装置的第二存储装置的步骤。

[0009] 在上述任一确认方法中,还可以具有:从待确认装置接收被使用第一私钥加密的第二验证信息的步骤。在上述任一确认方法中,还可以具有使用与第一私钥对应的第一公钥对加密的第二验证信息解密的步骤。在上述任一确认方法中,还可以具有:从待确认装置接收未被加密的所述第二验证信息的步骤。在上述任一确认方法中,还可以具有判定未被加密的第二验证信息和解密的第二验证信息是否一致的步骤。生成所述第三验证信息的步骤中,可以包含:在进行判定的步骤中判定为未被加密的第二验证信息以及解密的第二验证信息一致的情况下,基于第二验证信息对第一验证信息进行变换而生成第三验证信息的步骤。在上述任一确认方法中,还可以具有:从待确认装置获取使用第一私钥签名的第二验证信息的步骤。在上述任一确认方法中,还可以具有使用与第一私钥对应的第一公钥对签名进行验证的步骤。在上述任一确认方法中,获取签名的第二验证信息的步骤可以包含:获取使用第一私钥加密的第二验证信息和未被加密的第二验证信息的步骤。在上述任一确认方法中,对签名进行验证的步骤可以包含:使用第一公钥对加密的第二验证信息进行解密的步骤。在上述任一确认方法中,对签名进行验证的步骤可以包含判定未被加密的第二验证信息和解密的第二验证信息是否一致的步骤。在上述任一确认方法中,生成第三验证信息的步骤可以包含:在进行判定的步骤中判定为未被加密的第二验证信息以及解密的第二验证信息一致的情况下,基于第二验证信息对第一验证信息进行变换而生成第三验证信息的步骤。

[0010] 在上述任一确认方法中,第二验证信息是可以公钥。在上述任一确认方法中,第四验证信息可以是与公钥对应的私钥。在上述任一确认方法中,还可以具有:生成随机数的步骤。在上述任一确认方法中,还可以具有基于随机数来生成第一验证信息的步骤。

[0011] 在上述任一确认方法中,还可以具有:待确认装置从确认装置接收第一验证信息的步骤。在上述任一确认方法中,还可以具有待确认装置基于第一验证信息以及第四验证信息来生成第五验证信息的步骤。在上述任一确认方法中,可以还具有待确认装置将生成的第五验证信息向确认装置发送的步骤。

[0012] 在上述任一确认方法中,所述待确认装置可以具备蓄电装置。在上述任一确认方法中,确认装置可以具备构成为能够相对于待确认装置的蓄电装置进行拆装,并且使蓄电装置进行充电以及/或放电的充放电装置。在上述任一确认方法中,确认装置可以是具有第

一端子的第一电力装置。在上述任一确认方法中,待确认装置可以是具有构成为能够与第一端子进行安装的第二端子的第二电力装置。在上述任一确认方法中,还可以具有:在判定为第三验证信息以及第五验证信息不满足第二数学关系的情况下,或者在判定为第三验证信息以及第六验证信息不一致的情况下,决定禁止或者抑制第一电力装置以及第二电力装置之间的电力的输出输入的步骤。

[0013] 在上述任一确认方法中,确认装置可以是将待确认装置作为待保管装置进行保管的保管装置。在上述任一确认方法中,保管装置可以具有供待保管装置安装的安装部。在上述任一确认方法中,还可以具有:(a)在判定为第三验证信息以及第五验证信息不满足第二数学关系的情况下,或者在判定为第三验证信息以及第六验证信息不一致的情况下,决定不继续待保管装置相对于安装部的安装、或者以与合法装置不同的方式对待保管装置进行保管的步骤,以及/或者(b)在判定为第三验证信息以及第五验证信息满足第二数学关系的情况下,或者在判定为第三验证信息以及第六验证信息一致的情况下,决定继续待保管装置相对于安装部的安装、或者将待保管装置作为合法装置进行保管的步骤。

[0014] 在上述任一确认方法中,保管装置构成为能够对多个待保管装置的至少一个进行保管。在上述任一确认方法中,还可以具有:获取用于识别多个待保管装置中的能够被多个利用者共同利用的待保管装置的共同利用识别信息的步骤。在上述任一确认方法中,还可以具有在判定为第三验证信息以及第五验证信息满足第二数学关系的情况下,或者在判定为第三验证信息以及第六验证信息一致的情况下,基于共同利用识别信息,判定待确认装置是否是能够被多个利用者共同利用的待保管装置的步骤。在上述任一确认方法中,还可以具有(c)在判定为待确认装置不是能够被多个利用者共同利用的待保管装置的情况下,决定不继续待保管装置相对于安装部的安装、或者以与合法装置不同的方式对待保管装置进行保管,以及/或者(d)在判定为待确认装置是能够被多个利用者共同利用的待保管装置的情况下,决定继续待保管装置相对于安装部的安装、或者将待保管装置作为合法装置进行保管的步骤。

[0015] 在本发明的第二方式中,提供一种确认装置。上述确认装置例如确认待确认装置是否是合法装置。上述确认装置例如具备第一验证信息发送部,其将第一验证信息发送至待确认装置。上述确认装置例如具备第三验证信息生成部,其基于第二验证信息对第一验证信息进行变换而生成第三验证信息。上述确认装置例如具备响应接收部,其从待确认装置接收第五验证信息或第六验证信息,其中,(i)第五验证信息是待确认装置基于和第二验证信息满足第一数学关系的第四验证信息对第一验证信息进行变换而生成的信息,(i i)第六验证信息是待确认装置使用在待确认装置是合法装置时第三验证信息以及第五验证信息应该满足的第二数学关系,根据第一验证信息以及第四验证信息导出的、或根据第五验证信息导出的信息。上述确认装置例如具备判定部,其基于第三验证信息、以及第五验证信息或者第六验证信息,判定待确认装置是否是合法装置。在上述确认装置中,判定部例如进行如下处理:(a)在接收到第五验证信息的情况下,判定第三验证信息以及第五验证信息是否满足第二数学关系。在上述确认装置中,判定部例如(b)在接收到第六验证信息的情况下,判定第三验证信息以及第六验证信息是否一致。

[0016] 在本发明的第三方式中,提供一种蓄电装置。上述蓄电装置例如具备蓄电部,其蓄积电能。上述蓄电装置例如具备电端子,其用于与第一电力装置之间收发电力。在上述蓄电

装置中,第一电力装置例如对蓄电部充电。在上述蓄电装置中,第一电力装置例如利用蓄电部放电的电力。上述蓄电装置例如具备保存部,其保存第四验证信息。上述蓄电装置例如具备第一验证信息获取部,其从第一电力装置获取第一验证信息。上述蓄电装置例如具备响应部,其基于保存部所保存的第四验证信息,对第一验证信息获取部所获取的第一验证信息进行变换而生成第五验证信息,或者基于和第四验证信息满足第一数学关系的第二验证信息,生成对第一验证信息进行变换而得到的第六验证信息。

[0017] 在上述任一蓄电装置中,响应部可以将第五验证信息或者第六验证信息发送至第一电力装置。

[0018] 在本发明的第四方式中,提供一种确认系统。上述确认系统例如具备电力装置。在上述确认系统中,电力装置例如具有第二方式涉及的任一蓄电装置。上述确认系统例如具有第三方式涉及的任一蓄电装置。在上述确认系统中,确认装置例如确认为作为确认装置的确认对象亦即待确认装置的蓄电装置是合法装置。

[0019] 在本发明的第五方式中,提供一种程序。上述程序可以是用于使计算机执行上述第一方式涉及的任一确认方法的程序。上述程序可以是用于使计算机作为上述第二方式涉及的确认装置发挥功能的程序。上述程序可以是用于使计算机作为上述第三方式涉及的蓄电装置发挥功能的程序

[0020] 在本发明的第六方式中,提供一种计算机可读的存储介质。上述计算机可读的存储介质例如保存上述第五方式涉及的任一程序。上述计算机可读的存储介质可以是非易失性计算机可读介质。

[0021] 另外,上述发明的概述并没有列出本发明的所有特征。此外,这些特征组的子组合也可以是一项发明。

附图说明

[0022] 图1概略性地示出电池管理系统100的系统构成的一例。

[0023] 图2概略性地示出移动电池20的内部构成的一例。

[0024] 图3概略性地示出电池交换机120的内部构成的一例。

[0025] 图4概略性地示出移动电池20的认证流程的一例。

[0026] 图5概略性地示出电池认证部378的内部构成的一例。

[0027] 图6概略性地示出认证对应部232的内部构成的一例。

[0028] 图7概略性地示出搭载设备330的内部构成的一例。

[0029] 图8概略性地示出搭载设备370的内部构成的一例。

[0030] 图9概略性地示出移动电池920的内部构成的一例。

[0031] 图10概略性地示出认证用公钥74的获取流程的一例。

[0032] 图11概略性地示出认证用公钥74的获取流程的一例。

[0033] 图12概略性地示出移动电池20的认证流程的其他例子。

[0034] 图13概略性地示出响应码以及验证码的关系的一例。

[0035] 图14概略性地示出响应码以及验证码的验证流程的一例。

[0036] 图15概略性地示出响应码以及验证码的验证流程的其他例子。

[0037] 图16概略性地示出计算机5000的内部构成的一例。

具体实施方式

[0038] 以下,通过发明的实施方式来描述本发明,但以下实施方式不限定所要求保护的发明。此外,实施方式中描述的特征的所有组合对于本发明的解决方式不一定是必需的。另外,在附图中,有时对相同或类似的部分赋予相同的参照编号并省略了重复的说明。

[0039] (电池管理系统100的概要)

[0040] 图1概略性地示出电池管理系统100的系统构成的一例。在本实施方式中,电池管理系统100具备一个或多个(有时仅称为一个以上。)电池交换机120和管理服务器140。在本实施方式中,电池交换机120具有一个以上的保管单元122和通信单元126。在本实施方式中,保管单元122包含一个以上的槽124。在本实施方式中,通信单元126包含通信接口128。电池交换机120有时被称为电池站。

[0041] 在本实施方式中,电池管理系统100的各单元通过消耗从电力系统12接收的电力来操作。此外,电池管理系统100的每个单元可以经由通信网络14相互发送和接收信息。一个以上的保管单元122和通信单元126可以经由有线或无线的通信线路(未图示)彼此发送和接收信息。

[0042] 在本实施方式中,电池管理系统100管理一个或多个(有时称为一个以上)移动电池20。为了简化描述,在本实施方式中,将以电池管理系统100向电动自行车30的用户40提供移动电池20的共享服务的情况为示例来详细描述电池管理系统100。

[0043] 在本实施方式中,设置在电池交换机120的保管单元122中的一个以上的槽124中的每一个可以存储一个以上的移动电池20。此外,设置在电池交换机120的保管单元122中的一个以上的槽124中的每一个可以对一个以上的移动电池20充电。

[0044] 例如,加入移动电池20的共享服务的用户40使用通信终端42访问电池管理系统100,并请求借用移动电池20。用户40可以通过指定希望借出移动电池20的日期、时间和地点以及希望借出的移动电池20的数量来预约移动电池20的借出。通信终端42可以经由通信网络14访问电池管理系统100,也可以经由电池交换机120访问电池管理系统100。注意,用户40可以操作电池交换机120以请求借出移动电池20。

[0045] 当接收到上述请求时,用户40可以取出容纳在电池交换机120中的移动电池20(有时称为移动电池20的支出)。因此,用户40可以更换安装在电动自行车30上的移动电池20和容纳在电池交换机120中的移动电池20。

[0046] 更具体地说,用户40从电动自行车30移除安装在电动自行车30上的移动电池20。用户40将从电动自行车30移除的移动电池20归还到电池交换机120。当用户40归还移动电池20时,电池交换机120支出容纳在电池交换机120中的充电已完成的移动电池20。用户40从电池交换机120接收充电已完成的移动电池20,并将该充电已完成的移动电池20安装到电动自行车30上。由此,在电动自行车30和电池交换机120之间更换移动电池20。

[0047] 电池管理系统100中的移动电池20的认证

[0048] 在本实施方式中,电池交换机120可以设置在可上锁的建筑物或场地中,或者可以在未上锁的状态下设置在室外。考虑到用户40的便利性,电池交换机120优选地设置在多个用户40可自由使用的环境中。另一方面,当电池交换机120被设置在多个用户40可自由使用的环境中时,不受电池管理系统100管理的移动电池20(有时称为非正规的移动电池20)可能被插入到电池交换机120的槽124中。

[0049] 当规格与正规的移动电池20不同的非正规的移动电池20插入槽124中,并且该非正规的移动电池20的电端子和槽124的电端子安装在一起时,非正规的移动电池20的使用条件可能偏离适当范围。此外,由于电池交换机120被多个用户40使用,因此上述非正规的移动电池20可能被支出给与将非正规的移动电池20插入槽124的用户40不同的另一用户40。

[0050] 非正规的移动电池20不限于具有与由电池管理系统100管理的移动电池20(有时称为正规的移动电池20)不同规格的移动电池20。非正规的移动电池20可以具有与正规的移动电池20相同的规格,或者可以具有与正规的移动电池20对应的规格。

[0051] 例如,在电动自行车30的用户40购买移动电池20的情况下,如果用户40没有加入基于电池管理系统100的移动电池20的充电服务或移动电池20的交换服务,则用户40购买的移动电池20被视为具有与正规的移动电池20相同规格的非正规的移动电池20。根据本实施方式,电池管理系统100管理正规的移动电池20的劣化状态,并在适当的定时执行移动电池20的维护或交换。由此,用户40可以安全地使用移动电池20。此外,由于提供了劣化较小的移动电池20,因此改善了用户40的使用体验。

[0052] 另一方面,电池管理系统100不能掌握非正规的移动电池20的维护管理状态。因此,当维护管理不足的移动电池20混合在保管在电池交换机120中的移动电池20中时,用户40的使用体验可能会降低。因此,根据本实施方式,当移动电池20安装在槽124中时,电池交换机120执行移动电池20的认证处理。

[0053] 作为移动电池20的认证方法,包含(i)电动自行车30或电池交换机120获取作为认证对象的移动电池20的识别信息(有时称为电池ID),并将作为认证对象的移动电池20的电池ID与正规的移动电池20的电池ID的列表(有时称为白名单)进行比较的方法,以及(ii)电动自行车30或电池交换机120通过使用公共密钥加密方式发送和接收认证码来认证移动电池20的方法等。

[0054] 然而,根据上述方法,难以有效地抑制由于窃听、重复攻击等而导致的电池ID等的泄漏。例如,在使用电池ID的白名单认证移动电池20的情况下,如果在白名单中登记的电池ID泄漏,则难以抑制移动电池20的仿制品的流通。此外,在通过公共密钥加密方式认证移动电池20的情况下,当公共密钥泄漏时,难以抑制移动电池20的仿制品的流通。特别是,当多个电池的公共密钥相同时,由于模仿而造成的损害会增加。

[0055] 因此,在本实施方式中,电池管理系统100通过公钥加密方式认证移动电池20。由此,电池管理系统100在解决上述问题的同时,可以确认安装在槽124中的移动电池20是否是正规的移动电池20。

[0056] 此外,根据本实施方式,电池交换机120通过公钥加密方式认证移动电池20。作为公钥加密方式,可以采用公知的方式。作为公钥加密方式的密码,可以举例说明RSA密码、椭圆曲线密码等。

[0057] 由于安装在移动电池20或电动自行车30上的处理器的运算性能相对较低,因此难以在移动电池20或电动自行车30侧执行复杂的运算。另一方面,电池交换机120可以安装具有比安装在移动电池20或电动自行车30上的处理器更好的运算能力的处理器。与公共密钥加密方式相比,公钥加密方式的计算负荷较大。因此,在通过公钥加密方式认证移动电池20的情况下,执行该认证处理的处理器需要高速执行复杂的计算。关于这一点,电池交换机

120可以使用高性能处理器通过公钥加密方式来认证移动电池20。

[0058] 具体地说,首先,密钥发行者50为一个以上的移动电池20中的每一个发行一对认证私钥72和认证公钥74。密钥发行者50可以是移动电池20的制造商或转让人,可以是电池交换机120的制造商或转让人,或者可以是电池管理系统100的管理员或操作者。密钥发行者50可以是自然人、法人、组织、该法人或组织的成员、职员等。密钥发行者50可以使用通信终端52发行一对认证私钥72和认证公钥74。

[0059] 接着,密钥发行者50使一个以上的移动电池20中的每一个的认证私钥72存储在一个以上的移动电池20中的每一个的存储装置(未示出)中。在一个实施方式中,密钥发行者50可通信地连接通信终端52和移动电池20,并使通信终端52向移动电池20发送与连接到通信终端52的移动电池20相对应的认证私钥72。通信终端52和移动电池20可以通过有线通信或无线通信发送和接收信息。在另一实施方式中,密钥发行者50可以将认证私钥72输入到设置在移动电池20中的输入装置,或者可以将存储认证私钥72的存储装置安装在移动电池20上。

[0060] 此外,密钥发行者50将一个以上的移动电池20的认证公钥74存储在一个以上的电池交换机120的存储装置(未示出)中。在一个实施方式中,密钥发行者50将一个以上的移动电池20中的每一个的认证公钥74设置为可由一个以上的电池交换机120中的每一个获取的状态。例如,密钥发行者50操作通信终端52,设定使得一个以上的电池交换机120中的每一个能够访问数据库,该数据库针对一个以上的移动电池20中的每一个,相关联地存储电池ID和认证公钥74。上述数据库可以存储在通信终端52中,也可以存储在管理服务器140中。

[0061] 在另一实施方式中,密钥发行者50可通信地连接通信终端52和电池交换机120,并使上述数据库从通信终端52发送到电池交换机120。通信终端52和电池交换机120可以通过有线通信或无线通信发送和接收信息。在又一实施方式中,密钥发行者50可以从设置在电池交换机120中的输入装置输入上述数据库,或者可以将存储上述数据库的存储装置安装在电池交换机120上。在电池交换机120的制造、出厂、转移或安装时,上述数据库存储在电池交换机120的存储装置中。此外,可以适当地更新上述数据库。

[0062] 在该状态下,当用户40将移动电池20插入电池交换机120的槽124中并且移动电池20安装在槽124中时,电池交换机120首先获取安装在槽124中的移动电池20的电池ID。电池交换机120可以从移动电池20获取移动电池20的电池ID,或者可以从通信终端42获取移动电池20的电池ID。

[0063] 接下来,电池交换机120基于上述电池ID获取安装在槽124中的移动电池20的认证公钥74。在一个实施方式中,电池交换机120使用上述电池ID作为关键字,参考存储在电池交换机120的存储装置中的数据库,并获取安装在插槽124中的移动电池20的认证公钥74。在另一实施方式中,电池交换机120访问通信终端52或管理服务器140,使用上述电池ID作为关键字,参考存储在通信终端52或管理服务器140中的数据库,并获取安装在槽124中的移动电池20的认证公钥74。

[0064] 接下来,电池交换机120准备用于认证安装在槽124中的移动电池20的代码(有时称为认证码)。认证码可以是数字、字符和符号的组合。认证码可以是图像数据或音频数据。认证码可以在每次认证时生成,或者可以在每经过预定有效期时生成。认证码可以是为每个移动电池20预先确定的代码。例如,每当执行认证处理时,电池交换机120生成随机数,并

使用该随机数作为认证码。

[0065] 接下来,电池交换机120基于安装在槽124中的移动电池20的认证公钥74变换认证码。具体地说,电池交换机120使用安装在槽124中的移动电池20的认证公钥74来加密认证码。由此,生成包含加密认证码的质询码。

[0066] 电池交换机120将生成的质询码发送到移动电池20,并请求移动电池20响应该质询码。作为对质询码的响应,例示发送包含表示移动电池20成功解密用认证公钥74加密的认证码的信息的响应码。

[0067] 作为表示移动电池20成功解密用认证公钥74加密的认证码的信息,例示(i)解密的认证码和(ii)根据预定算法(有时称为第一算法)对解密的认证码进行信息处理而生成的信息等。第一算法的示例包含与使用预定函数(有时称为第一函数)的运算处理相关的算法、与使用预定信息的加密处理相关的算法等。作为上述函数,例示哈希函数。

[0068] 作为上述加密处理,可以是使用公共密钥的公共密钥方式的加密处理,或者可以是使用公钥和私钥的公钥方式的加密处理。作为公钥方式的加密处理,例示上述RSA密码、椭圆曲线密码等。

[0069] 当移动电池20接收到质询码和对质询码的响应请求(有时称为认证响应请求)时,使用移动电池20的认证私钥72对由认证公钥74加密的认证码进行解密。当移动电池20成功地解密用认证公钥74加密的认证码时,获得解密的认证码。由此,移动电池20可以使用质询码或包含在该质询码中的认证公钥74所加密的认证码和移动电池20的认证私钥72来生成解密的认证码。

[0070] 然后,移动电池20根据预定规则生成响应码。上述规则可以是表示表示移动电池20成功地解密由认证公钥74加密的认证码的信息的类型或生成流程的信息。此外,移动电池20将生成的响应码作为对认证响应请求的响应发送到电池交换机120。

[0071] 在一个实施方式中,上述规则表示使用解密的认证码作为表示移动电池20成功解密由认证公钥74加密的认证码的信息。在这种情况下,移动电池20生成包含解密的认证码的响应码。

[0072] 在另一实施方式中,上述规则表示使用通过根据第一算法对解密的认证码进行信息处理而生成的信息(有时称为解密的认证码的第一处理值)作为表示移动电池20成功解密用认证公钥74加密的认证码的信息。在这种情况下,移动电池20通过根据第一算法对解密的认证码执行信息处理来生成上述第一处理值。此外,移动电池20生成包含上述第一处理值的响应码。通过使用包含上述第一处理值的响应码,可以抑制由于窃听、重复攻击等而导致的认证码的泄漏、认证算法的反向分析等。

[0073] 例如,在第一算法是与使用哈希函数的运算处理相关的算法的情况下,移动电池20生成包含解密的认证码的哈希值的响应码。当第一算法是使用公共密钥的公共密钥方式的加密处理时,移动电池20生成包含通过使用公共密钥对解密的认证码进行加密而获得的密文的响应码。当第一算法是使用公钥和私钥的公钥方式的加密处理时,移动电池20生成包含通过使用私钥或公钥对解密的认证码进行加密而获得的密文的响应码。

[0074] 接下来,电池交换机120从移动电池20接收响应码。基于上述响应码,电池交换机120确认移动电池20成功地解密了用认证公钥74加密的认证码。

[0075] 在一个实施方式中,当上述响应码包含解密的认证码时,电池交换机120将由电池

交换机120生成的认证码与包含在响应码中的认证码进行比较。例如,电池交换机120判定由电池交换机120生成的认证码是否与包含在响应码中的认证码匹配。此外,电池交换机120基于比较结果确认移动电池20是否成功地解密了由认证公钥74加密的认证码。由此,电池交换机120可以确认安装在槽124中的移动电池20是否是正规的移动电池20。

[0076] 例如,当由电池交换机120生成的认证码与包含在响应码中的复原的认证码匹配时,电池交换机120确认安装在槽124中的移动电池20是正规的移动电池20。另一方面,当由电池交换机120生成的认证码与包含在响应码中的复原的认证码不匹配时,电池交换机120确认安装在槽124中的移动电池20不是正规的移动电池20,或者安装在槽124中的移动电池20是非正规的移动电池20。

[0077] 在另一实施方式中,当上述响应码包含解密的认证码的第一处理值时,电池交换机120将通过根据第一算法对由电池交换机120生成的认证码进行信息处理而生成的信息(有时称为由电池交换机120生成的认证码的第一处理值)与包含在响应码中的解密的认证码的第一处理值进行比较。例如,电池交换机120判定由电池交换机120生成的认证码的第一处理值是否与上述解密的认证码的第一处理值匹配。此外,电池交换机120基于比较结果确认移动电池20是否成功地解密了由认证公钥74加密的认证码。由此,电池交换机120可以确认安装在槽124中的移动电池20是否是正规的移动电池20。

[0078] 例如,当由电池交换机120生成的认证码的第一处理值与包含在响应码中的复原的认证码的第一处理值匹配时,电池交换机120确认安装在槽124中的移动电池20是正规的移动电池20。另一方面,当由电池交换机120生成的认证码的第一处理值与包含在响应码中的复原的认证码的第一处理值不匹配时,电池交换机120确认安装在槽124中的移动电池20不是正规的移动电池20,或者安装在槽124中的移动电池20是非正规的移动电池20。

[0079] 在又一实施方式中,当上述响应码包含解密的认证码的第一处理值时,电池交换机120将由电池交换机120生成的认证码与通过根据第二算法对包含在响应码中的解密的认证码的第一处理值进行信息处理而生成的信息(有时称为复原的认证码的第二处理值)进行比较。例如,电池交换机120判定由电池交换机120生成的认证码是否与上述解密的认证码的第二处理值匹配。此外,电池交换机120基于比较结果确认移动电池20是否成功地解密了由认证公钥74加密的认证码。由此,电池交换机120可以确认安装在槽124中的移动电池20是否是正规的移动电池20。

[0080] 第二算法可以是与使用作为第一函数的逆函数的第二函数的运算处理有关的算法,或者与用于对由第一算法的加密处理加密的信息进行解密的解密处理有关的算法。上述解密处理可以是使用用于加密第一算法的密钥信息或与该密钥信息配对的密钥信息的解密处理。

[0081] 例如,当由电池交换机120生成的认证码与包含在响应码中的复原的认证码的第二处理值匹配时,电池交换机120确认安装在槽124中的移动电池20是正规的移动电池20。另一方面,当由电池交换机120生成的认证码与包含在响应码中的复原的认证码的第二处理值不匹配时,电池交换机120确认安装在槽124中的移动电池20不是正规的移动电池20,或者安装在槽124中的移动电池20是非正规的移动电池20。

[0082] 如上所述,电池交换机120可以确认移动电池20是正规的移动电池20,同时有效地抑制认证码的泄漏。此外,电池交换机120可以确认安装在槽124中的移动电池20不是正规

的移动电池20,或者安装在槽124中的移动电池20是非正规的移动电池20,同时有效地抑制例如认证码那样的用于认证合法装置的信息的泄漏。

[0083] 如上所述,电池交换机120被配置为能够交换移动电池20。因此,电池交换机120可以基于上述确认结果来确定是否交换移动电池20。电池交换机120可以基于用于识别多个移动电池20中可共同使用的移动电池20的信息(有时称为白名单)来判定是否交换移动电池20。电池交换机120可以基于上述确认结果和白名单来判定是否交换移动电池20。

[0084] 类似地,电池交换机120被配置为能够对移动电池20充电或放电。因此,电池交换机120可以基于上述确认结果来判定移动电池20是否充电或放电。电池交换机120可以基于白名单来判定移动电池20是否充电或放电。电池交换机120可以基于上述确认结果和白名单来判定移动电池20是否充电或放电。

[0085] 与电池管理系统100相关的每个单元的概述

[0086] 在本实施方式中,通信网络14发送信息。通信网络14可以是有线通信的传输线、无线通信的传输线或无线通信的传输线和有线通信的传输线的组合。通信网络14可以包含无线分组通信网络、因特网、P2P网络、专用线路、VPN、电力线通信线路等。

[0087] 通信网络14可以包含(i)诸如蜂窝电话线网络的移动通信网络和(ii)诸如无线MAN(例如,WiMAX(注册商标))、无线LAN(例如,WiFi(注册商标))、蓝牙(注册商标)、Zigbee(注册商标)和NFC(Near Field Communication)等的无线通信网络。无线LAN、蓝牙(注册商标)、Zigbee(注册商标)和NFC可以是短距离无线通信的示例。

[0088] 在本实施方式中,移动电池20蓄积电能。移动电池20可以被配置为可拆装地连接到电动自行车30(有时称为可拆装)。移动电池20可以被配置为可拆装地连接到电池交换机120。由此,用户40可以交换安装在电动自行车30上的移动电池20和容纳在电池交换机120中的移动电池20。

[0089] 在一个实施方式中,移动电池20安装在电动自行车30上并向电动自行车30供电。如上所述,移动电池20可以可拆装地安装到电动自行车30上。在另一实施方式中,当移动电池20容纳在电池交换机120中时,移动电池20由电池交换机120充电。

[0090] 注意,当移动电池20容纳在电池交换机120中时,移动电池20可以向电池交换机120供电。由此,电池交换机120可以将容纳在电池交换机120中的移动电池20的一部分用作例如不间断电源装置(有时称为UPS)。

[0091] 在本实施方式中,移动电池20存储认证私钥72。认证私钥72可以存储在设置在移动电池20中的任何类型的存储装置(未示出)中。移动电池20可以存储用于与电池交换机120执行的各种加密处理和/或解密处理的各种密钥。上述密钥的示例包含用于电子签名的私钥,用于电子签名的公钥等。

[0092] 在本实施方式中,电动自行车30搭载有移动电池20。电动自行车30可以搭载多个移动电池20。电动自行车30使用存储在移动电池20中的电力。例如,电动自行车30消耗从移动电池20提供的电力来行驶。

[0093] 在本实施方式中,通信终端42经由通信网络14向电池管理系统100的每个单元发送和接收信息。当用户40访问电池管理系统100时,通信终端42可以用作用户接口。通信终端42可以用于电池管理系统100的用户认证处理。

[0094] 通信终端42的示例包含个人计算机、便携式终端等。作为便携式终端,例示包含移

动电话、智能手机、PDA、平板电脑、笔记本电脑或膝上型计算机、可穿戴计算机等。

[0095] 在本实施方式中,通信终端52经由通信网络14向电池管理系统100的每个单元发送和接收信息。当密钥发行者50访问电池管理系统100时,通信终端52可以用作用户接口。

[0096] 通信终端52可以用于生成诸如认证私钥72和认证公钥74的各种密钥的处理。通信终端52可以将生成的认证私钥72存储在与该密钥相对应的移动电池20的存储装置中。在认证私钥72存储在移动电池20中之后,通信终端52可以从通信终端52的存储装置中擦除认证私钥72。通信终端52可以将生成的认证公钥74存储在一个以上的电池交换机120的存储装置中。对于一个以上的移动电池20中的每一个,通信终端52可以具有将电池ID与上述各种公钥相关联地存储的数据库。上述数据库可以将一个以上的移动电池20中的每一个的电池ID和一个以上的移动电池20中的每一个的认证公钥74相关联地存储。

[0097] 通信终端52可以被配置为能够与一个以上的电池交换机120进行无线通信。通信终端52可以是已经确认一个以上的电池交换机120中的至少一个正规的信息处理装置。通信终端52可以是对于一个以上的电池交换机120能够信赖的信息处理装置。通信终端52可以被配置为能够与一个以上的移动电池20进行无线通信。通信终端52可以是已经确认一个以上的移动电池20中的至少一个正规的信息处理装置。通信终端52可以是对于一个以上的移动电池20能够信赖的信息处理装置。

[0098] 通信终端52的示例包含个人计算机、便携式终端等。便携式终端的示例包含移动电话、智能手机、PDA、平板电脑、笔记本电脑或膝上型计算机、可穿戴计算机等。

[0099] 在本实施方式中,电池交换机120容纳移动电池20。电池交换机120可以容纳多个移动电池20。由此,电池交换机120可以保管一个以上的移动电池20。在本实施方式中,电池交换机120对一个以上的移动电池20中的至少一个充电。电池交换机120可以对移动电池20充电,直到移动电池20的充电率或电压达到预定设置值。

[0100] 在本实施方式中,电池交换机120使充电完成的移动电池20处于可取出状态(有时称为支出)。电池交换机120可以响应于来自用户40的请求而支出与该请求匹配的移动电池20。电池交换机120可以从管理服务器140获取表示作为与要支出的移动电池20相关的条件的支出条件的信息,并从满足该支出条件的移动电池20中确定实际要支出的移动电池20。

[0101] 注意,在另一实施方式中,电池交换机120可以使多个移动电池20的至少一部分放电。电池交换机120可以使用通过移动电池20的放电输出的电力。例如,电池交换机120通过消耗由移动电池20的放电输出的电力来操作。当电池交换机120通过消耗由一个移动电池20的放电输出的电力来操作时,可以停止或中断另一个移动电池20的充电操作。即使在这种情况下,电池交换机120也可以继续移动电池20的支出操作。

[0102] 由此,电池交换机120可以使用容纳在电池交换机120中的移动电池20的一部分作为不间断电源装置。根据本实施方式的电池交换机120,例如,即使在从电力系统12向电池交换机120的电力供应中发生异常的情况下,也可以继续向控制装置供电。结果,例如,电池交换机120可以继续支出移动电池20。因此,即使在例如电池交换机120安装在停电发生频率相对较高的区域中的情况下,也可以提供能够稳定地交换电池的环境。

[0103] 在本实施方式中,保管单元122保持多个槽124。在本实施方式中,保管单元122独立于通信单元126形成。保管单元122可以与通信单元126分离地安装,或者可以与通信单元126邻接地安装。

[0104] 此外,在本实施方式中,保管单元122基于从通信单元126发送的第一命令生成包含用于控制多个槽124中的至少一个的操作的一个以上的过程的处理流。对于一个以上的处理中的每一个,保管单元122判定是否可以执行每个处理。对于判定为可执行的处理,保管单元122生成用于控制作为该处理的对象的槽124的第二命令。保管单元122基于生成的第二命令来控制上述槽124的操作。由此,可以限制由第一命令表示的指令的一部分的执行。

[0105] 例如,在上述一个以上的处理包含与移动电池20的安全或用户40或电池交换机120的维护人员的安全相关的操作的情况下,保管单元122确定是否满足允许执行与安全相关的操作的条件。当确定满足上述条件时,保管单元122确定可以执行该处理。由此,基于与上述处理有关的第二命令来控制槽124的操作。另一方面,当确定不满足上述条件时,保管单元122确定不能执行该处理。在这种情况下,与上述处理有关的第二命令不被发送到槽124。

[0106] 由此,即使在通信单元126基于来自管理服务器140的请求输出第一命令的情况下,也可以确保移动电池20、用户40或上述维护人员的安全。例如,即使在管理服务器140发送上述请求之后电池交换机120的状态发生变化的情况下,当电池交换机120的通信环境良好时,管理服务器140也可以取消上述请求。然而,也要考虑到在电池交换机120的通信环境不令人满意的情况下,管理服务器140需要花费时间才能取消上述请求。根据本实施方式,由于保管单元122根据电池交换机120的状态确定是否可以执行第二命令,所以电池交换机120可以停止或中断部分处理的执行,而无需等待来自管理服务器140的取消请求。

[0107] 在本实施方式中,多个槽124中的每一个被配置为能够保管一个以上的移动电池20中的至少一个。一个以上的移动电池20中的至少一个安装在多个槽124中的每一个上。此外,多个槽124中的每一个具备电连接到一个以上的移动电池20的电端子(未示出)的电端子(未示出)。由此,多个槽124中的每一个可以对保管在每个槽中的移动电池20充电或放电。

[0108] 注意,“电连接”不限于两个元件直接物理连接的情况。第三元件可以插入上述两个元素之间。此外,上述两个元件物理连接的情况不受限制。例如,变压器的输入绕组和输出绕组不是物理连接的,而是电连接的。由此,在槽124中,不仅可以支持移动电池20的有线充放电,还可以支持移动电池20的无线充放电。

[0109] 多个槽124中的每一个可以具备可通信地连接到一个以上的移动电池20的通信端子的通信端子。槽124的通信端子和移动电池20的通信端子之间的通信方法可以是有线通信方法或无线通信方法。由此,多个槽124中的每一个可以从保管在每个槽中的移动电池20的存储装置(未示出)读取信息或将信息写入该存储装置。

[0110] 在本实施方式中,通信单元126负责在电池交换机120中的信息处理中涉及用户40和管理服务器140中的至少一个的信息处理。例如,通信单元126从用户40和管理服务器140中的至少一个接收请求,并响应该请求。当通信单元126判断为为了处理来自用户40和管理服务器140中的至少一个的请求需要保管单元122时,通信单元126向保管单元122发送命令(有时称为指令)。上述第一命令可以是命令的示例。

[0111] 当通信单元126可以在不与保管单元122协作的情况下处理来自用户40和管理服务器140中的至少一个的请求时,通信单元126可以不向保管单元122发送命令。由此,简化

了保管单元122中的信息处理。例如,通信单元126可以在不与保管单元122协作的情况下执行与电池交换机120外部的通信控制处理、用户40的认证处理、槽124的选择处理等。

[0112] 如上所述,在本实施方式中,通信单元126独立于保管单元122形成。保管单元122可以与通信单元126分离地安装,或者可以与通信单元126邻接地安装。

[0113] 通信接口128被配置为能够与电池交换机120外部的信息处理装置通信。通信接口128可以支持多种通信方式。通信接口128可以支持有线通信方式或无线通信方式。在一个实施方式中,通信接口128与用户40使用的通信终端42之间发送和接收信息。在另一实施方式中,通信接口128与管理服务器140之间发送和接收信息。

[0114] 在本实施方式中,管理服务器140设置在电池交换机120的外部。此外,管理服务器140可以经由通信网络14与电池交换机120的通信单元126之间发送和接收信息。

[0115] 在本实施方式中,管理服务器140管理一个以上的移动电池20。例如,管理服务器140管理一个以上的移动电池20中的每一个的状态。管理服务器140可以管理一个以上的移动电池20中的每一个的返还和支出。管理服务器140可以向一个以上的电池交换机120中的至少一个发送用于管理移动电池20的各种请求。

[0116] 管理服务器140可以管理一个以上的电池交换机120。管理服务器140可以管理一个以上的电池交换机120中的每一个的状态。作为电池交换机120的状态,例示外部电力的供应状态、可接受的移动电池20的数量、可支出的移动电池20的数量、可用作不间断电源的移动电池20的有无、其数量或其识别信息、上述移动电池20的充电状态等。管理服务器140可以向一个以上的电池交换机120中的至少一个发送用于管理电池交换机120的各种请求。

[0117] 管理服务器140可以为一个以上的电池交换机120中的至少一部分确定支出条件,该支出条件是与作为支出对象的移动电池20相关的条件。作为支出条件,例示了与容纳在电池交换机120中的多个移动电池20中的每一个的支出相关的优先级、要优先支出的移动电池20的识别信息、要优先支出的移动电池20的特征等。

[0118] 在本实施方式中,管理服务器140可以用于诸如认证公钥74的各种密钥的分发处理。管理服务器140可以具有数据库,该数据库针对一个以上的移动电池20中的每一个,将电池ID和上述各种密钥相关联地存储。上述数据库可以将一个以上的移动电池20中的每一个的电池ID和一个以上的移动电池20中的每一个的认证公钥74相关联地存储。管理服务器140可以根据来自一个以上的电池交换机120中的每一个的请求提取由该请求表示的移动电池20的认证公钥74,并发送提取的认证公钥74。

[0119] 管理服务器140可以被配置为能够与一个以上的电池交换机120进行无线通信。管理服务器140可以是已经确认一个以上的电池交换机120中的至少一个正规的信息处理装置。管理服务器140可以是对于一个以上的电池交换机120能够信赖的信息处理装置。管理服务器140可以被配置为能够与一个以上的移动电池20进行无线通信。管理服务器140可以是已经确认一个以上的移动电池20中的至少一个是正规的信息处理装置。管理服务器140可以是对于一个以上的移动电池20能够信赖的信息处理装置。

[0120] 移动电池20可以是待确认装置、第二电力装置或蓄电装置的示例。密钥发行者50可以是确认装置的制造商或转让者、待确认装置的制造商或转让者、第二信息和第四信息的发行者的示例。通信终端52可以是第一外部装置或第二外部装置的示例。电池管理系统100可以是确认装置或确认系统的示例。电池交换机120可以是确认装置、第一电力装置或

保管装置的示例。保管单元122可以是第一电力装置或保管装置的示例。槽124可以是第一电力装置、保管装置或安装部的示例。管理服务器140可以是第一外部装置或第二外部装置的示例。

[0121] 认证码可以是第一信息的示例。认证公钥74可以是第二信息的示例。由认证公钥74加密的认证码可以是第三信息的示例。质询码可以是第三信息的示例。认证私钥72可以是第四信息的示例。解密的认证码可以是第五信息的示例。解密的认证码的第一处理值可以是第六信息的示例。由电池交换机120生成的认证码的第一处理值可以是第七信息的示例。复原的认证码的第二处理值可以是第八信息的示例。用于第一算法的加密处理的信息可以是第九信息的示例。用于第二算法的解密处理的信息可以是第九信息或第十信息的示例。

[0122] 加密可以是信息的变换的示例。解密可以是信息的逆变换的示例。正规的移动电池20可以是合法装置的示例。非正规的移动电池20可以是非合法装置的示例。白名单可以是共同利用识别信息的示例。认证移动电池20的方法可以是移动电池20的确认方法的示例。

[0123] 认证码可以是第一验证信息的示例。认证公钥74可以是第二验证信息的示例。用认证公钥74加密的认证码可以是第三验证信息的示例。认证私钥72可以是第四验证信息的示例。认证私钥72可以是第一私钥的示例。认证公钥74可以是与第一私钥相对应的第一公钥的示例。

[0124] 另一实施方式的示例

[0125] 在本实施方式中,以电池管理系统100提供移动电池20的共享服务的情况为例详细描述了电池管理系统100。然而,由电池管理系统100提供的服务不限于本实施方式。在另一实施方式中,电池管理系统100可以向移动电池20的用户40提供移动电池20的充电服务。

[0126] 在本实施方式中,以电池交换机120使用从电力系统12接收的电力来操作的情况为例详细描述了电池交换机120。然而,电池交换机120不限于本实施方式。在另一实施方式中,例如,当设置在电池交换机120中的一个以上的槽124中的至少一个包含双向DC/DC变换器时,电池交换机120可以使用从保管在电池交换机120中的一个以上的移动电池20中的至少一个放电的电力来操作。

[0127] 在本实施方式中,以电池交换机120包含一个以上的保管单元122和单个通信单元126的情况为例详细描述了电池管理系统100。然而,电池交换机120不限于本实施方式。在另一实施方式中,电池交换机120可以包含多个保管单元122和多个通信单元126。在这种情况下,保管单元122的数量可以大于通信单元126的数量。

[0128] 在本实施方式中,以一个以上的电池交换机120中的每一个从密钥发行者50、通信终端52或管理服务器140获取一个以上的移动电池20的认证公钥74的情况为例,详细描述了电池管理系统100。然而,电池交换机120中的认证公钥74的获取方法不限于本实施方式。在另一实施方式中,一个以上的电池交换机120中的每一个可以从安装在槽124中的移动电池20获取该移动电池的认证公钥74。

[0129] 在本实施方式中,以(i)电池交换机120生成认证码,(ii)电池交换机120用认证公钥74加密生成的认证码以生成质询码,(iii)移动电池20用认证私钥72解密包含在质询码中的加密的认证码以生成响应码的情况为例,描述了用于认证移动电池20的方法的示例。

然而,用于认证移动电池20的方法不限于本实施方式。根据另一实施方式,使用电子签名或电子证书来认证移动电池20。使用电子签名的认证过程的示例如下所示。

[0130] 例如,移动电池20首先生成认证码。接下来,移动电池20使用私钥对认证码进行签名。具体地说,移动电池20使用私钥对认证码进行加密。此时,移动电池20可以使用私钥对包含认证码和从电池交换机120发送的信息和/或临时信息(例如,表示签名时的时间的时间信息)的数据(有时称为消息)进行加密。由此,抑制了重复攻击造成的损害。

[0131] 例如,移动电池20将电池ID、生成的认证码(明文)和加密的信息(有时称为密文)相关联地发送到电池交换机120。如上所述,密文可以是上述认证码被加密的数据。密文可以是上述消息被加密的数据。

[0132] 接下来,当电池交换机120从移动电池20接收到上述数据时,电池交换机120执行用于获取移动电池20的公钥的处理。例如,电池交换机120访问存储在任意存储装置中的公钥的数据库,以获取与移动电池20的电池ID相关联的公钥。电池交换机120使用移动电池20的公钥对包含在从移动电池20接收的数据中的认证码的密文进行解密。

[0133] 电池交换机120将上述解密的认证码与从移动电池20接收的认证码(明文)进行比较。例如,电池交换机120判定上述解密的认证码与从移动电池20接收的认证码(明文)是否匹配。当两者匹配时,电池交换机120确认移动电池20是真实的。

[0134] 在本实施方式中,以生成包含加密的认证码的质询码的情况为例,描述了确认装置认证待确认装置的方法的示例。然而,质询码不限于本实施方式。在另一实施方式中,质询码可以包含未加密的认证码。

[0135] 关于确认处理的主体的另一实施方式的示例

[0136] 在本实施方式中,以电池交换机120认证移动电池20的情况为例,详细描述用于确认装置确认待确认装置是否是合法装置的确认方法。然而,确认方法不限于本实施方式。

[0137] 熟悉本说明书的描述的本领域技术人员可以理解,无论确认装置和待确认装置的具体组合如何,确认装置可以通过与电池交换机120确认移动电池20的过程相同的过程来确认待确认装置。例如,在确认装置是移动电池20并且待确认装置是电池交换机120的情况下,移动电池20可以通过与电池交换机120确认移动电池20的过程相同的过程来确认电池交换机120是否是合法装置。

[0138] 例如,确认装置不限于电池交换机120。认证移动电池20的主体可以是(i)被配置为可电连接到移动电池20的装置,(ii)被配置为可向移动电池20供电的装置,或(iii)被配置为可从移动电池20接收电力的装置(这些装置有时被称为电力装置)。类似地,待确认装置不限于移动电池20。例如,在移动电池20认证另一装置的情况下,由移动电池20认证的对象可以是(i)被配置为可电连接到移动电池20的装置,(ii)被配置为可向移动电池20供电的装置或(iii)被配置为可从移动电池20接收电力的装置(这些装置有时被称为电力装置)。

[0139] 电力装置的示例包含电动自行车30、电池交换机120等。电力装置的另一示例包含(a)具有移动电池20的充电功能但不具有向外部供电功能的充电器,(b)安装有一个以上的移动电池20并向外部供电存储在一个以上的移动电池20中的电力的供电装置,以及(c)具有移动电池20的充电功能(或从外部接收电力的功能)和移动电池20的放电功能(或向外部供电的功能)两者的功能的装置。

[0140] 在另一实施方式中,确认装置可以是移动电池20,待确认装置可以是电动自行车30、通信终端52或电池交换机120。在又一实施方式中,确认装置可以是电动自行车30,待确认装置可以是移动电池20。在又一实施方式中,确认装置可以是电池交换机120,待确认装置可以是通信终端52或管理服务器140。在又一实施方式中,确认装置可以是通信终端52,待确认装置可以是移动电池20、电池交换机120或管理服务器140。在又一实施方式中,确认装置可以是管理服务器140,待确认装置可以是通信终端52或电池交换机120。在又一实施方式中,在移动电池20和管理服务器140可以相互发送和接收信息的情况下,确认装置是移动电池20,待确认装置可以是管理服务器140。此外,确认装置可以是管理服务器140,待确认装置可以是移动电池20。

[0141] 如上所述,移动电池20可以是确认装置的示例。电池交换机120可以是待确认装置的示例。电动自行车30可以是确认装置或待确认装置的示例。正规的电池交换机120可以是合法装置的示例。正规的电动自行车30可以是合法装置的示例。用于一个装置认证另一个装置的认证方法可以是确认方法的示例。不是合法装置的电池交换机120(有时称为非正规的电池交换机120)可以是非合法装置的示例。不是合法装置的电动自行车30(有时称为非正规的电动自行车30)可以是非合法装置的示例。

[0142] 确认装置可以是第一装置和第二装置中的一个的示例,并且待确认装置可以是第一装置和第二装置中的另一个的示例。确认装置可以是信息处理装置和其他信息处理装置中的一个的示例,并且待确认装置可以是信息处理装置和其他信息处理装置中的另一个的示例。

[0143] 电力装置可以是设备的示例。移动电池20的存储装置可以是存储部的示例。

[0144] 图2概略性地示出了移动电池20的内部构成的示例。在本实施方式中,移动电池20具备电力连接器212、通信连接器214、蓄电部220、控制部230、认证对应部232、感测部240和保存部250。在本实施方式中,保存部250包含电池ID保存部252和认证私钥保存部254。

[0145] 在本实施方式中,电力连接器212包含用于在与槽124或电动自行车30之间发送和接收电力的电端子。在本实施方式中,通信连接器214包含用于在与槽124或电动自行车30之间发送和接收信息的通信端子。在本实施方式中,蓄电部220包含用于蓄积电能的蓄电单元。

[0146] 在本实施方式中,控制部230控制移动电池20的操作。当移动电池20保管在槽124中时,控制部230可以在与保管单元122之间发送和接收信息。

[0147] 在本实施方式中,认证对应部232对应来自电池交换机120的认证响应请求。例如,当移动电池20安装在电池交换机120的一个槽124中时,认证对应部232从电池交换机120接收质询码和认证响应请求。认证对应部232响应于认证响应请求向电池交换机120发送响应码。稍后将描述认证对应部232的细节。

[0148] 在本实施方式中,感测部240获取表示移动电池20的状态的信息。感测部240可以包含多种类型的传感器。感测部240中包含的传感器的示例包含温度传感器、电压传感器、电流传感器等。

[0149] 保存部250保存关于移动电池20的各种信息。例如,保存部250保存移动电池20的识别信息。保存部250可以保存与移动电池20电连接的电动自行车30、电池交换机120或槽124的识别信息。保存部250可以保存移动电池20的操作历史。例如,保存部250将时间与感

测部240的测量结果相关联地存储作为移动电池20的操作历史。

[0150] 在本实施方式中,电池ID保存部252保存移动电池20的电池ID。在本实施方式中,认证私钥保存部254保存移动电池20的认证私钥72。

[0151] 电力连接器212可以是电端子或第二端子的示例。蓄电部220可以是蓄电装置的示例。认证私钥存储部254可以是保存部的示例。认证对应部232可以是第三信息获取部、第五信息生成部或响应部的示例。保存部250可以是存储部的示例。信息的保存可以是信息的存储的示例。

[0152] 图3概略性地示出了电池交换机120的内部配置的示例。在本实施方式中,电池交换机120包含一个以上的保管单元122、通信单元126、通信线路310、不间断电源装置312和路由器314。在本实施方式中,一个以上的保管单元122中的每一个包含壳体320和搭载设备330。在本实施方式中,搭载设备330包含一个以上的槽124、感测部332、设定保存部334和控制部336。在本实施方式中,通信单元126包含壳体360和搭载设备370。在本实施方式中,搭载设备370包含通信接口128、用户接口372、用户识别部374、控制部376和电池认证部378。

[0153] 在本实施方式中,一个以上的槽124中的每一个被配置为可拆卸地连接到移动电池20。此外,一个以上的槽124中的每一个向移动电池20供电,并对移动电池20的蓄电部220充电。一个以上的槽124中的每一个可以接收从移动电池20输出的电力。

[0154] 在本实施方式中,通信线路310将一个以上的保管单元122中的每一个连接到通信单元126。在本实施方式中,不间断电源装置312设置在电力系统12和通信单元126之间。例如,当来自电力系统12的电力供应发生异常时,不间断电源装置312向通信部126供电。在本实施方式中,路由器314中继或转发通信单元126和通信网络14之间的通信。

[0155] 在本实施方式中,壳体320保持搭载设备330。壳体320的形状和材料没有特别限制。壳体320可以具有箱形、板形或框架的形状。

[0156] 在本实施方式中,搭载设备330搭载在壳体320上。搭载设备330的搭载模式没有特别限制。搭载设备330可以容纳在壳体320的内部,或者可以安装在壳体320的表面上。

[0157] 在本实施方式中,感测部332获取表示槽124或保管在槽124中的移动电池20的状态的信息。感测部332可以包含多种类型的传感器。感测部240中包含的传感器的示例包含温度传感器、电压传感器、电流传感器等。

[0158] 在本实施方式中,设定保存部334保存与保管单元122相关的各种设定。设定保存部334可以包含物理开关或任何类型的存储介质,例如存储器或硬盘。上述设定可以由(i)物理开关的开/关来表示,或者(ii)可以作为电子数据存储在存储介质中。上述设定的示例包含关于保管单元122的ID的设定、关于保管单元122的设置位置的设定、关于保管单元122中的各种操作的执行可否的设定等。

[0159] 在本实施方式中,控制部336控制保管单元122的操作。上述操作的示例包含移动电池20相对于槽124的安装或拆卸、移动电池20的充电或放电等。

[0160] 在一个实施方式中,控制部336控制移动电池20相对于槽124的安装或移除。作为上述控制,例示设置在槽124中的闸门(未示出)的锁定控制、设置在槽124中的移除防止构件(未示出)的控制、用于约束设置在槽124中的移动电池20的机构(未示出)的控制、设置在槽124中的可移动连接器(未示出)的控制等。可移动连接器可以是机械连接器或电动连接器。

[0161] 在另一实施方式中,控制部336控制保管在槽124中的移动电池20的充电或放电。上述控制的示例包含电端子的连接确认、调整充电电压、调整充电电流、调整放电电压、调整放电电流等。由此,可以控制经由电端子的移动电池20的充电或放电。

[0162] 控制部336可以基于从控制部376接收的命令来控制保管单元122的操作。例如,基于从控制部376接收的命令,控制部336生成包含用于控制多个槽124中的至少一个的操作的一个以上的过程的处理流。对于一个以上的处理中的每一个,控制部336判定是否可以执行每个处理。控制部336针对判定为可执行的处理生成命令,并将该命令发送到作为控制对象的槽124。另一方面,对于被判定为不可执行的处理,不生成和发送上述命令。

[0163] 控制部336可以将表示基于从控制部376接收的命令的操作的执行结果的信息向控制部376发送。例如,控制部336向控制部376发送表示保管单元122是否根据从控制部376接收的命令执行了操作的信息。

[0164] 在本实施方式中,壳体360保持搭载设备370。壳体360的形状和材料没有特别限制。壳体360可以具有箱形、板形或框架的形状。

[0165] 在本实施方式中,搭载设备370搭载在壳体360上。搭载设备370的搭载模式没有特别限制。搭载设备370可以容纳在壳体360的内部,或者可以安装在壳体360的表面上。

[0166] 在本实施方式中,用户接口372向使用电池交换机120的用户40提供各种信息。此外,用户接口372接受来自使用电池交换机120的用户40的输入。用户接口372的示例包含显示器、扬声器、键盘、指向装置、触摸面板、麦克风、照相机、语音输入系统、手势输入系统等。

[0167] 在本实施方式中,用户识别部374识别使用电池交换机120的用户40。作为识别用户40的方法,可以采用公知的方法。例如,用户识别部374通过分析用户40的图像并执行用户40的认证处理来识别用户40。用户识别部374可以通过使用用户40持有的ID卡执行用户40的认证处理来识别用户40。用户识别部374可以通过使用用户40携带的通信终端42执行用户40的认证处理来识别用户40。

[0168] 在本实施方式中,控制部376负责在电池交换机120中的信息处理中涉及用户40和管理服务器140中的至少一个的信息处理。例如,控制部376从用户40和管理服务器140中的至少一个接收请求,并响应该请求。当控制部376判断为为了处理来自用户40和管理服务器140中的至少一个的请求需要保管单元122时,控制部376向保管单元122发送命令(例如,上述第一命令)。

[0169] 当控制部376可以在不与保管单元122协作的情况下处理来自用户40和管理服务器140中的至少一个的请求时,控制部376可以不向保管单元122发送命令。例如,控制器376可以在不与保管单元122协作的情况下执行与电池交换机120的外部的通信控制处理、用户40的认证处理、槽124的选择处理等。

[0170] 更具体地说,当控制部376从用户40和管理服务器140中的至少一个接收请求时,控制部376首先生成包含用于处理该请求的一个以上的过程的处理流。接下来,控制部376从上述一个以上的处理中提取包含保管单元122中的处理的处理。控制部376为每个提取的处理生成表示保管单元122中的处理的内容的命令。

[0171] 上述命令可以包含表示作为控制对象的保管单元122(有时称为对象单元)的信息。上述命令可以包含表示作为控制对象的槽124(有时称为对象槽)的信息。上述命令可以包含对象槽的识别信息和表示对象槽中的操作内容的信息。

[0172] 此后,控制部376将上述命令发送到作为命令对象的保管单元122。控制部376可以从接收到上述命令的保管单元122获取表示针对上述命令的执行结果的信息。

[0173] 控制部376可以基于电池认证部378的输出来确定移动电池20的保管模式。控制部376可以基于电池认证部378的认证结果来确定移动电池20的充电模式。控制部376可以基于电池认证部378的认证结果来确定移动电池20的放电模式。

[0174] 如后文所述,电池认证部378例如输出表示特定的移动电池20是否是合法装置的信息。例如,电池认证部378输出表示是否继续将特定的移动电池20安装到槽124的信息。例如,电池认证部378输出表示特定的移动电池20是否以与合法装置不同的方式保管的信息。例如,电池认证部378输出表示特定的移动电池20是否作为合法装置被保管的信息。例如,电池认证部378输出表示是否执行特定的移动电池20的充电和/或放电的信息。例如,电池认证部378输出表示特定的移动电池20的认证处理失败的信息。

[0175] 当控制部376获取了表示特定的移动电池20不是合法装置的信息时,控制部376可以禁止该特定的移动电池20的充电,或者可以不允许特定的移动电池20的充电。在特定的移动电池20不是合法装置的情况下,控制部376可以控制特定的移动电池20的充电,使得充电电流或充电功率的允许值小于特定的移动电池20是合法装置的情况。在特定的移动电池20不是合法装置的情况下,控制部376可以允许该特定的移动电池20放电,也可以不禁止该放电。在特定的移动电池20不是合法装置的情况下,控制部376可以控制特定的移动电池20的放电,使得放电电流或放电功率的允许值小于特定的移动电池20是合法装置的情况。

[0176] 在另一实施方式中,当确认装置是电动自行车30并且待确认装置是移动电池20时,电动自行车30的计算机可以用作控制部376和电池认证部378。在这种情况下,上述移动电池20的充电可以通过再生电力进行。

[0177] 当控制部376获取了表示特定的移动电池20的认证处理失败的信息时,控制部376可以执行与未判定移动电池20是合法装置的情况相同的处理。当控制部376获取了表示特定的移动电池20的认证处理失败的信息时,电池认证部378可以确定以不同于合法装置的方式保管移动电池20。例如,电池认证部378仅在满足特殊条件的时间段内保管移动电池20。上述期间的示例包含直到移动电池20的管理者回收移动电池20的期间、例如由于非常态或紧急情况的发生而放松移动电池20的支出条件的期间。

[0178] 当控制部376获取了表示特定的移动电池20的认证处理失败的信息时,控制部376可以禁止该特定的移动电池20的充电,或者可以不允许该特定的移动电池20的充电。当特定的移动电池20的认证处理失败时,控制部376可以控制特定的移动电池20的充电,使得充电电流或充电功率的允许值小于该特定的移动电池20的认证处理成功时的允许值。当控制部376获取了表示特定的移动电池20的认证处理失败的信息时,控制部376可以禁止该特定的移动电池20的放电,或者可以不允许该特定的移动电池20的放电。当特定的移动电池20的认证处理失败时,控制部376可以控制特定的移动电池20的放电,使得放电电流或放电功率的允许值小于该特定的移动电池20的认证处理成功时的允许值。

[0179] 当控制部376获取了表示特定的移动电池20的认证处理失败的信息时,控制部376可以访问该特定的移动电池20的保存部250,以获取存储在保存部250中的特定的信息。例如,控制部376可以访问特定的移动电池20的保存部250,以获取在该特定的移动电池20安装到当前电池交换机120之前安装的电池交换机120(有时称为紧前的电池交换机120)的识

别信息。例如,控制部376可以访问特定的移动电池20的保存部250,以获取在该特定的移动电池20安装到当前电池交换机120之前安装的电力装置(电池交换机120以外的电力装置。例如电动自行车30。)的识别信息。

[0180] 控制部376可以将上述紧前的电池交换机120的识别信息和/或上述电力装置的识别信息发送到管理服务器140。由此,管理服务器140可以检测上述紧前的电池交换机120的故障或异常。管理服务器140可以基于上述电力装置的识别信息和该电力装置的移动历史或电池交换历史来确定上述紧前的电池交换机120。

[0181] 电池认证部378执行移动电池20的认证处理。例如,电池认证部378确认安装在槽124中的移动电池20是否是正规的移动电池20。当特定的移动电池20的认证处理失败时,电池认证部378可以重新执行特定的移动电池20的认证处理。可以预先确定重新执行的次数。重新执行的模式没有特别限制,可以从认证码的生成开始重新执行,或者可以使用先前生成的认证码重新执行认证处理。电池认证部378的细节将在后面描述。

[0182] 电池认证部378可以是确认装置的示例。槽124可以是充电装置的示例。槽124可以是充放电装置的示例。

[0183] 将参考图4、图5和图6详细描述电池交换机120中的移动电池20的认证处理的示例。图4概略性地示出了移动电池20的认证过程的示例。图5概略性地示出了用于实现参考图4描述的认证过程的电池认证部378的内部配置的示例。图6概略性地示出了用于实现参考图4描述的认证过程的认证对应部232的内部配置的示例。注意,电池交换机120中的移动电池20的认证处理、认证对应部232和电池认证部378不限于本实施方式。

[0184] 在参考图4描述的实施方式中,以移动电池20已经完成从密钥发行者50、通信终端52或管理服务器140获取移动电池20的认证私钥72的步骤的情况为例来描述移动电池20的认证处理的示例。在上述获取处理中,移动电池20例如将认证私钥72存储在认证私钥保存部254中。

[0185] 此外,在参考图4描述的实施方式中,以电池交换机120已经完成从密钥发行者50、通信终端52或管理服务器140获取与上述一个以上的移动电池20的认证公钥74相关的数据库的步骤的情况为例来描述移动电池20的认证处理的示例。在上述获取处理中,电池交换机120将与一个以上的移动电池20的认证公钥74相关的数据库存储在例如设置在电池认证部378或搭载设备370中的存储装置中。

[0186] 在本实施方式中,在移动电池20的认证处理开始的阶段,移动电池20的认证私钥72存储在认证私钥保存部254中。类似地,电池交换器120的电池认证部378包含一个以上的移动电池20的认证公钥74有关的数据库。

[0187] 如图4所示,根据本实施方式,首先,在步骤420(步骤有时缩写为S)中,电池交换机120的电池认证部378检测移动电池20安装在槽124中。当电池交换机120的电池认证部378检测到移动电池20安装在槽124中时,电池交换机120的电池认证部378向移动电池20发送激活信号。

[0188] 在S422中,当移动电池20的控制部230接收到激活信号时,例如,控制部230和认证对应部232被激活。此时,控制部230可以向电池交换部120发送表示认证对应部232已经被激活的激活确认信号。

[0189] 接下来,在S424中,电池认证部378向移动电池20发送请求发送电池ID的信号(有

时称为ID发送请求)。例如,在S426中,当移动电池20的控制部230接收到ID发送请求信号时,控制部230将存储在电池ID保存部252中的电池ID发送到电池交换机120。

[0190] 接下来,在S430中,当电池认证部378获取移动电池20的电池ID时,电池认证部378使用该电池ID作为关键字参考与上述认证公钥74相关的数据库,并提取与该电池ID匹配的认证公钥74。当没有提取到与电池ID匹配的认证公钥74时,电池认证部378可以访问通信终端52或管理服务器140,以获取与电池ID匹配的认证公钥74。

[0191] 此外,电池认证部378准备认证码。例如,电池认证部378生成随机数,并确定使用该随机数作为认证码。

[0192] 接下来,电池认证部378基于移动电池20的认证公钥74变换认证码,并生成包含变换后的认证码的质询码。例如,电池认证部378使用移动电池20的认证公钥74对认证码进行加密。此外,电池认证部378生成包含加密的认证码的质询码。

[0193] 此外,在本实施方式中,电池认证部378准备验证码。例如,电池认证部378执行使用了哈希函数的运算处理,以生成认证码的哈希值。电池认证部378确定使用生成的哈希值作为验证码。

[0194] 接下来,在S432中,电池认证部378向移动电池20发送质询码。电池认证部378可以向移动电池20发送质询码和认证响应请求。

[0195] 在S434中,当认证对应部232接收到质询码时,认证对应部232基于存储在认证私钥保存部254中的认证私钥72反向变换包含在质询码中的加密的认证码。具体地,认证对应部232使用存储在认证私钥保存部254中的认证私钥72来解密包含在质询码中的加密认证码。由于认证私钥72与认证公钥74配对,所以如果移动电池20是正规的移动电池20,则认证对应部232成功地解密加密的认证码。

[0196] 接下来,在S436中,认证对应部232生成响应码,该响应码包含表示移动电池20成功地解密了用认证公钥74加密的认证码的信息。例如,认证对应部232执行使用了哈希函数的运算处理,以生成解密的认证码的哈希值。认证对应部232生成包含解密的认证码的哈希值的响应码。此外,认证对应部232将响应码发送到电池交换机120。

[0197] 接下来,在S438中,当电池认证部378接收到响应码时,电池认证部378将包含在响应码中的哈希值与作为验证码生成的哈希值进行比较。例如,电池认证部378确定包含在响应码中的哈希值是否与作为验证码生成的哈希值匹配。此外,在S440中,基于上述比较结果,电池认证部378确定移动电池20是否是正规的移动电池20(有时称为合法装置)。

[0198] 根据本实施方式,在S450中,电池认证部378可以基于S440中的判定结果来判定是否交换移动电池20。例如,在没有判定移动电池20是合法装置的情况下,电池认证部378确定不将移动电池20安装到槽124中。

[0199] 上述安装可以不包含用于认证处理的临时安装。例如,当电池交换机120和移动电池20通过有线通信时,移动电池20可以临时安装在电池交换机120上,以便电池认证部378认证移动电池20。例如,上述安装意味着移动电池20继续安装在电池交换机120上。上述安装可以意味着移动电池20被作为合法装置保管。

[0200] 在一个实施方式中,当没有判定为移动电池20是合法装置时,电池认证部378可以确定不继续将移动电池20安装到槽124中。在没有判定为移动电池20是正规的移动电池20的情况下,电池认证部378可以确定以与合法装置不同的方式保管移动电池20。例如,电池

认证部378仅在满足特殊条件的时间段内保管移动电池20。上述期间的示例包含直到移动电池20的管理者回收移动电池20的期间、例如由于非常态或紧急情况的发生而放松移动电池20的支出条件的期间。

[0201] 在另一实施方式中,当判定为移动电池20是合法装置时,电池认证部378确定将移动电池20安装到槽124中。当判定为移动电池20是合法装置时,电池认证部378可以确定继续将移动电池20安装到槽124中。当判定为移动电池20是合法装置时,电池认证部378可以确定将移动电池20作为合法装置保管。

[0202] 电池认证部378可以基于S440中的判定结果和上述白名单来判定是否交换移动电池20。例如,当判定为移动电池20是正规的移动电池20时,电池认证部378判定移动电池20是否是可由多个用户40使用的移动电池20。

[0203] 具体地,电池认证部378确认上述移动电池20的电池ID是否公开在白名单中。当上述移动电池20的电池ID被公开在白名单中时,电池认证部378判定为移动电池20是可由多个用户40使用的移动电池20。另一方面,在上述移动电池20的电池ID没有公开在白名单中的情况下,电池认证部378判定为移动电池20不是可由多个用户40使用的移动电池20。

[0204] 当判定为移动电池20不是可由多个用户40使用的移动电池20时,电池认证部378可以确定不将移动电池20安装到槽124中。由此,例如,即使移动电池20是正规的移动电池20,当移动电池20的用户40没有加入基于电池管理系统100的移动电池20的充电服务或移动电池20的交换服务时,也抑制了上述移动电池20保管在电池交换机120中。

[0205] 当确定移动电池20不被安装到槽124时,即使为了执行移动电池20的认证处理而将移动电池20安装到槽124中,电池交换机120也可以解除移动电池20的安装,并将移动电池20返回给用户40。另外,移动电池20安装在槽124中的方式没有特别限制。可以是移动电池20容纳在槽124的内部的方式,或者可以是移动电池20放置在槽124上的方式。

[0206] 在确定不继续将移动电池20安装到槽124的情况下,可以执行与确定不将移动电池20安装到槽124的情况相同的信息处理。当确定移动电池20以与合法装置不同的方式保管时,可以执行与确定移动电池20不安装到槽124的情况相同的信息处理。

[0207] 此外,根据本实施方式,在S450中,电池认证部378可以基于S440中的判定来判定移动电池20是否被充电和/或放电。例如,在没有判定为移动电池20是正规的移动电池20的情况下,确定不对移动电池20进行充电和/或放电。由此,可以禁止或抑制槽124和移动电池20之间的电力的输入/输出。电池认证部378可以基于S440中的判定结果和上述白名单,通过与上述过程类似的过程来判定移动电池20是否充电和/或放电。

[0208] 另外,移动电池20中的处理可以由单个处理器执行,或者可以由多个处理器协作执行。类似地,电池交换机120中的处理可以由单个处理器执行,或者可以由多个处理器协作执行。这进一步提高了安全性。

[0209] 例如,移动电池20包含用于控制移动电池20的各种操作的控制CPU和用于执行加密处理和解密处理的安全IC。S422和S426由上述控制CPU执行。此外,在S434中,当控制CPU接收到质询码时,控制CPU将质询码传送到安全IC。安全IC在S434中解密质询码,并在S436中生成响应码。此外,在S436中,安全IC将生成的响应码输出到控制CPU。在S436中,控制CPU将由安全IC生成的响应码发送到电池交换机120。

[0210] 判定或确认移动电池20不是合法装置的情况可以是未判定移动电池20是合法装

置的情况的示例。判定或确认移动电池20是非正规的移动电池20的情况可以是未判定移动电池20是合法装置的情况的示例。

[0211] 未判定为移动电池20是合法装置的情况可以是判定为第三验证信息和第五验证信息不满足第二数学关系的情况的示例,或者第三验证信息和第六验证信息不匹配的情况的示例。判定为移动电池20是合法装置的情况可以是判定为第三验证信息和第五验证信息满足第二数学关系的情况的示例,或者第三验证信息和第六验证信息匹配的情况的示例。

[0212] 如图5所示,在本实施方式中,电池认证部378包含保存部520、电池ID获取部530、认证码生成部540、验证码生成部550、质询码生成部560、质询码发送部562、响应码获取部570、比较部582和判定部584。在本实施方式中,保存部520包含公钥数据库522和白名单524。

[0213] 在本实施方式中,保存部520存储各种信息。在本实施方式中,公钥数据库522关联地存储由电池管理系统100管理的一个以上的移动电池20中的每一个的电池ID和上述一个以上的移动电池20中的每一个的认证公钥74。白名单524保存由电池管理系统100管理的一个以上的移动电池20的电池ID。在另一实施方式中,公钥数据库522可以用作白名单524。

[0214] 在一个实施方式中,电池认证部378从密钥发行者50获取公钥数据库522。电池认证部378将从密钥发行者50获取的公钥数据库522保存在保存部520中。在另一实施方式中,电池认证部378从通信终端52或管理服务器140获取公钥数据库522。电池认证部378将从通信终端52或管理服务器140获取的公钥数据库522保存在保存部520中。

[0215] 在本实施方式中,电池ID获取部530获取容纳在槽124中的移动电池20的电池ID或容纳在槽124中的移动电池20的电池ID。电池ID获取部530可以获取安装在槽124中的移动电池20的电池ID。电池ID获取部530可以从通信终端42或移动电池20获取上述移动电池20的电池ID。

[0216] 在本实施方式中,认证码生成部540生成认证码502。认证码生成部540可以通过生成随机数来生成认证码502。

[0217] 在本实施方式中,验证码生成部550生成验证码。验证码生成部550根据移动电池20生成响应码的规则来生成验证码。当生成包含由移动电池20复原的认证码本身的响应码时,验证码生成部550可以不生成验证码,也可以确定使用认证码作为验证码。

[0218] 在本实施方式中,验证码生成部550执行使用了哈希函数552的运算处理,以生成认证码502的哈希值504。验证码生成部550确定使用生成的哈希值504作为验证码。验证码生成部550将上述哈希值504作为验证码输出到比较部582。

[0219] 在本实施方式中,质询码生成部560生成质询码512。例如,质询码生成部560使用移动电池20的认证公钥74对认证码502进行加密。由此,电池认证部378可以生成包含加密的认证码502的质询码512。

[0220] 在本实施方式中,质询码发送部562将由质询码发送部562生成的质询码512发送到移动电池20。质询码发送部562可以向移动电池20发送质询码512和认证响应请求。

[0221] 在本实施方式中,响应码获取部570从移动电池20获取与质询码512相对应的响应码516。在本实施方式中,响应码516包含在移动电池20中复原的认证码502的哈希值506。响应码获取部570将复原的认证码502的哈希值506输出到比较部582。

[0222] 在本实施方式中,比较部582从验证码生成部550获取作为验证码的哈希值504。此

外,比较部582从响应码获取部570获取包含在响应码516中的哈希值506。比较部582将作为验证码的哈希值504与包含在响应码516中的哈希值506进行比较。例如,比较部582判定作为验证码的哈希值504和包含在响应码516中的哈希值506是否匹配。比较部582将表示比较结果的信息输出到判定部584。

[0223] 在本实施方式中,判定部584获取表示比较部582的比较结果的信息。判定部584基于比较部582的比较结果来判定移动电池20是否是正规的移动电池20。

[0224] 判定部584可以基于关于移动电池20是否是正规的移动电池20的判定结果来判定是否交换移动电池20。判定部584可以基于关于移动电池20是否是正规的移动电池20的确定结果和白名单524来判定是否交换移动电池20。

[0225] 判定部584可以基于关于移动电池20是否是正规的移动电池20的判定结果来判定移动电池20是否被充电和/或放电。由此,可以禁止或抑制槽124和移动电池20之间的电力输入/输出。判定部584可以基于关于移动电池20是否是正规的移动电池20的判定结果和白名单524来判定移动电池20是否被充电和/或放电。

[0226] 保存部520可以是第一存储装置的示例。质询码生成部560可以是第三信息生成部的示例。质询码发送部562可以是第三信息发送部的示例。响应码获取部570可以是响应接收部的示例。比较部582可以是比较部的示例。

[0227] 如图6所示。在本实施方式中,认证对应部232包含请求接收部620、ID发送部630、质询码获取部640、质询码解密部650、响应码生成部660和响应码发送部670。

[0228] 在本实施方式中,请求接收部620从电池交换机120接收各种类型的请求。上述请求的示例包含ID发送请求、认证响应请求等。在本实施方式中,当请求接收部620从电池交换机120接收到ID发送请求时,ID发送部630将移动电池20的电池ID发送到电池交换机120。

[0229] 在本实施方式中,当请求接收部620从电池交换机120接收到认证响应请求时,质询码获取部640获取由电池交换机120发送的质询码512。在本实施方式中,质询码解密部650使用认证私钥72对包含在质询码512中的加密的认证码502进行解密。此外,质询码解密部650将解密后的认证码502输出到响应码生成部660。

[0230] 在本实施方式中,响应码生成部660基于解密的认证码502生成响应码516。响应码生成部660可以根据上述规则生成任意格式的响应码516。

[0231] 根据本实施方式,响应码生成部660执行使用了哈希函数662的运算处理,以生成复原的认证码502的哈希值506。响应码生成部660生成包含复原的认证码502的哈希值506的响应码516。在本实施方式中,响应码发送部670将响应码516发送到电池交换机120。

[0232] 质询码获取部640可以是第三信息获取部的示例。质询码解密部650可以是第五信息生成部的示例。响应码发送部670可以是响应部的示例。

[0233] 另一实施方式的示例

[0234] 在本实施方式中,以在图4的S450中判定为安装在槽124中的移动电池20不是可由多个用户40使用的移动电池20的情况下,电池认证部378确定不将移动电池20安装在槽124中或者不对移动电池20进行充电或放电的情况为例,描述了电池交换机120中的信息处理的示例。然而,当判定为不是可由多个用户40使用的移动电池20时的信息处理不限于本实施方式。在另一实施方式中,当判定为不是可由多个用户40使用的移动电池20时,电池认证部378可以根据预定的第一规则执行将移动电池20安装到槽124的处理,也可以根据预定的

第二规则执行移动电池20的充电处理或放电处理。

[0235] 作为第一规则,例示允许将移动电池20安装在槽124中,但不允许将移动电池20安装在槽124中的用户40以外的用户40取出上述移动电池20的规则。作为第二规则,例示允许移动电池20充电或放电,直到移动电池20安装在槽124上的次数达到预定的次数或频度,但是当移动电池20安装在槽124上的次数超过上述的次数或频度时,不允许移动电池20充电或放电的规则。

[0236] 在本实施方式中,以电池交换机120从密钥发行者50、通信终端52或管理服务器140获取移动电池20的认证公钥74的情况为例,描述了移动电池20的认证处理的示例。然而,电池交换机120中的认证公钥74的获取方法不限于本实施方式。在另一实施方式中,电池交换机120可以从移动电池20获取认证公钥74。

[0237] 在本实施方式中,以通过将从认证码生成的验证码与响应码进行比较来执行认证码和响应码的比较处理的情况为例,描述了移动电池20的认证处理的示例。然而,比较认证码和响应码的处理不限于本实施方式。可以通过结合图1描述的各种方法来比较认证码和响应码。

[0238] 图7概略性地示出了搭载设备330的内部配置的示例。在本实施方式中,为了简化描述,将使用槽124不具有对移动电池20放电的功能的情况作为示例来详细描述搭载设备330。然而,熟悉本申请说明书的描述的本领域技术人员可以理解,槽124可以被改变为能够对移动电池20进行充电/放电的配置。

[0239] 在本实施方式中,搭载设备330包含一个以上的槽124、断路器710、电力线712、AC/DC电源714、分配器716、电力线718、主控板730、通信集线器732、通信线路734、温度调节部742、蜂鸣器744、感测部746和维护门748。在本实施方式中,槽124包含AC/DC充电器760、电力连接器762、槽控制板770、通信连接器772、驱动部774、闸门776、锁定部778、温度调节部782、状态显示部784和感测部786。

[0240] 在本实施方式中,断路器710从电力系统12接收电力。断路器710经由电力线712将从电力系统12接收的电力提供给一个以上的槽124中的每一个的AC/DC充电器760。断路器710将从电力系统12接收的电力提供给AC/DC电源714。断路器710的示例包含电路断路器、具有过电流保护的剩余电流断路器等。

[0241] 在本实施方式中,AC/DC电源714用作提供控制电力的电源。例如,AC/DC电源714将从断路器710接收的交流电力变换为具有适当电压的直流电力。AC/DC电源714经由分配器716和电力线718向一个以上的槽124中的每一个的槽控制板770提供变换后的直流电力。此外,AC/DC电源714向主控板730提供变换后的直流电力。

[0242] 在本实施方式中,主控板730控制保管单元122的每个单元的操作。主控板730经由通信线路310连接到CPU板820。主控板730可以用作控制部336。主控板730可以与槽控制板770协作地用作控制部336。

[0243] 主控板730经由通信集线器732和通信线路734与一个以上的槽124中的每一个的槽控制板770之间发送和接收信息。主控板730可以控制温度调节部742、蜂鸣器744、感测部746和维护门748的操作。主控板730可以获取表示温度控制部742、蜂鸣器744、感测部746和维护门748的状态的信息。

[0244] 例如,主控板730从感测部746获取表示感测部746的测量结果的信息。此外,主控

板730从维护门748获取表示维护门748的打开/关闭状态的信息。

[0245] 在本实施方式中,温度调节部742调节保管单元122的壳体320的内部的温度。温度调节部742的示例包含风扇、水冷式冷却器等。

[0246] 在本实施方式中,蜂鸣器744向用户40通知保管单元122的状态。蜂鸣器744可以输出警告声音。蜂鸣器744可以从具有不同警告模式的多个警告声音中输出由主控板730指定的警告。

[0247] 在本实施方式中,感测部746获取表示保管单元122的状态的信息。感测部746可以包含多种类型的传感器。感测部746中包含的传感器的示例包含温度传感器、振动传感器、漏电传感器等。感测部746可以构成感测部332的至少一部分。

[0248] 在本实施方式中,维护门748设置在壳体320的开口部(未示出),并用于电池交换机120的维护人员对电池交换机120的维护管理。维护门748可以向主控板730输出表示打开/关闭状态的信息。例如,当维护门748打开时,维护门748输出表示维护门748已经打开的信号。

[0249] 在本实施方式中,AC/DC充电器760对电连接到电力连接器762的移动电池20充电。AC/DC充电器760根据来自槽控制板770的指令调整施加到电连接到电力连接器762的移动电池20的电压和电流中的至少一个。

[0250] 在本实施方式中,电力连接器762包含当移动电池20容纳在槽124中时电连接到移动电池20的电力连接器212的电端子。在本实施方式中,电力连接器762被配置为可由驱动部774移动。另外,在另一实施方式中,电力连接器762可以固定在槽124的内部。

[0251] 在本实施方式中,槽控制板770控制槽124的每个单元的操作。槽控制板770可以根据来自主控板730的指令来控制槽124的操作。槽控制板770可以用作控制部336。槽控制板770可以与主控板730协作地用作控制部336。

[0252] 槽控制板770可以经由通信连接器772与保管在槽124中的移动电池20的控制部230之间发送和接收信息。例如,槽控制板770可以读取存储在移动电池20的保存部250中的信息。此外,槽控制板770可以将信息写入移动电池20的保存部250。

[0253] 在本实施方式中,通信连接器772包含当移动电池20容纳在槽124中时可通信地连接到移动电池20的通信连接器214的通信端子。在本实施方式中,通信连接器772被配置为可由驱动部774移动。另外,在另一实施方式中,通信连接器772可以固定在槽124的内部。

[0254] 在本实施方式中,驱动部774驱动设置在槽124中的各种可移动构件。驱动部774可以根据来自槽控制板770的指令驱动上述可移动构件。可移动构件的示例包含电力连接器762、通信连接器772、闸门776、锁定部778、设置在槽124中的移除防止构件、用于约束设置在槽124中的移动电池20的机构等。

[0255] 在本实施方式中,闸门776设置在槽124的开口部(未示出),并控制用户40对移动电池20的可用与否。闸门776可以根据来自槽控制板770的指令来控制其打开/关闭。

[0256] 例如,当闸门776处于打开状态时,用户40可以将移动电池20插入槽124中或从槽124取出移动电池20。另一方面,当闸门776处于关闭状态时,移动电池20不能插入槽124中或从槽124中取出。

[0257] 在本实施方式中,锁定部778在闸门776的锁定状态和解锁状态之间切换。锁定部778可以根据来自槽控制板770的指令在闸门776的锁定状态和解锁状态之间切换。

[0258] 在本实施方式中,温度调节器782调节槽124内的温度。在本实施方式中,温度调节部782可以根据来自槽控制板770的指令来调节槽124内的温度。温度控制部782的示例包含风扇、水冷式冷却器等。

[0259] 在本实施方式中,状态显示部784向用户40通知槽124的状态。槽124的状态的例示包含移动电池20的有无,异常的有无等。例如,状态显示部784可以通过多个点亮图案、闪烁图案或显示图案中的被槽控制板770指定的点亮图案、闪烁图案或显示图案来向用户40通知槽124的状态。状态显示部784的示例包含LED、显示器等。

[0260] 在本实施方式中,感测部786获取表示槽124的状态的信息。感测部786可以包含多种类型的传感器。感测部786中包含的传感器的示例包含温度传感器、电压传感器、电流传感器等。例如,感测部786包含(i)用于测量槽124内部或移动电池20附近的温度的温度传感器、(ii)用于测量电力连接器762的电压的电压传感器和(iii)用于测量流过电力连接器762的电流的电流传感器中的至少一个。感测部786可以构成感测部332的至少一部分。

[0261] 主控板730可以是确认装置的示例。电力连接器762可以是第一端子的示例。槽控制板770可以是确认装置的示例。

[0262] 图8概略性地示出了搭载设备370的内部配置的示例。在本实施方式中,搭载设备370包含AC/DC电源814、服务插座816、CPU板820、作为以太网(注册商标)的通信接口的以太网接口(以太网I/F)830、NFC读取器842、照相机844、触摸面板852、显示器854和扬声器856。

[0263] 在本实施方式中,AC/DC电源814、AC/DC电源714用作提供控制电力的电源。AC/DC电源814例如经由不间断电源装置312从电力系统12接收电力。AC/DC电源814将从电力系统12接收的交流电力变换为具有适当电压的直流电力。AC/DC电源814向CPU板820提供变换后的直流电力。

[0264] 在本实施方式中,服务插座816向通信部126外部的设备供电。外部的设备的示例是路由器314。

[0265] 服务插座816例如经由不间断电源装置312从电力系统12接收电力。服务插座816可以根据来自CPU板820的指令控制对外部的设备的电力供应。服务插座816可以将关于提供给外部的设备的电力的信息发送到CPU板820。

[0266] CPU板820控制通信单元126的每个单元的操作。CPU板820经由通信线路310连接到主控板730。CPU板820可以用作控制部376。

[0267] 在本实施方式中,以太网接口830经由路由器314连接到通信网络14。以太网接口830可以用作通信接口128。

[0268] 在本实施方式中,NFC读取器842经由短距离无线通信与通信终端42之间发送和接收信息。NFC读取器842可以用作通信接口128。NFC读取器842可以用作用户识别部374。

[0269] 在本实施方式中,照相机844拍摄用户40。相机844可以用作用户接口372。相机844可以用作用户识别部374。

[0270] 在本实施方式中,触摸面板852接受来自用户40的触摸输入。触摸面板852可以用作用户接口372。在本实施方式中,显示器854通过输出图像向用户40呈现信息。显示器854可以用作用户接口372。在本实施方式中,扬声器856通过输出声音向用户40呈现信息。扬声器856可以用作用户接口372。

[0271] CPU板820可以是确认装置的示例。触摸面板852可以是上述输入装置的示例。

[0272] 参考图9、图10和图11,将描述电池交换机120获取认证公钥74的过程的另一示例。图9概略性地示出了移动电池920的内部配置的示例。图10概略性地示出了认证公钥74的获取过程的示例。图11概略性地示出了认证公钥74的获取过程的示例。

[0273] 在参考图1至图6描述的实施方式中,以电池交换机120从密钥发行者50、通信终端52或管理服务器140获取存储一个以上的移动电池20的认证公钥74的数据库的情况为例,详细描述了电池管理系统100。根据结合图9、图10和图11描述的实施方式,与结合图1至图6描述的实施方式的不同之处在于,电池交换机120从安装在槽124中的移动电池20获取该移动电池20的认证公钥74。关于上述差异以外的特征,参考图9、图10和图11描述的实施方式可以具有与参考图1至图6描述的实施方式相同的配置。

[0274] 如图9所示,在本实施方式中,移动电池920与移动电池20的不同之处在于,保存部250包含电池ID保存部252、认证私钥保存部254、认证公钥保存部955、签名私钥保存部956和签名验证公钥保存部957。除了上述差异之外,移动电池920可以具有与移动电池20相同的配置。

[0275] 在参考图9描述的实施方式中,移动电池920可以不包含签名验证公钥84和签名验证公钥保存部957。例如,在电池交换机120存储移动电池920的签名验证公钥84的情况下,或者电池交换机120可以获取移动电池920的签名验证公钥84的情况下,移动电池920可以不包含签名验证公钥84和签名验证公钥保存部957。

[0276] 移动电池920可以不包含签名私钥82和签名私钥保存部956。在这种情况下,例如,移动电池920可以在设置在移动电池920中的任何存储装置中存储(i)用签名私钥82加密的认证公钥74、(ii)用签名私钥82加密了认证公钥74和任意信息的信息、以及(iii)认证公钥74的电子证书中的至少一个。

[0277] 用签名私钥82加密的认证公钥74、以及用签名私钥82加密了认证公钥74和任意信息的信息有时被称为电子签名。例如,使用椭圆曲线密码进行数字签名的一系列流程称为椭圆曲线数字签名算法。

[0278] 认证公钥74的电子证书例如包含认证公钥74和用签名私钥82加密的认证公钥74。认证公钥74的电子证书例如包含认证公钥74(或认证用公钥74和任意信息)、用签名私钥82加密了认证公钥74和该任意信息的信息。注意,在参考图1至图6描述的实施方式中,移动电池920与参考图9描述的实施方式的不同之处在于,移动电池920不包含签名私钥82和签名私钥保存部956、以及签名验证公钥84和签名验证公钥保存部957。

[0279] 在本实施方式中,认证公钥保存部955存储认证公钥74。在本实施方式中,签名私钥保存部956存储移动电池20用于提供电子签名的签名私钥82。签名验证公钥保存部957存储签名验证公钥84,其用于电池交换机120验证包含移动电池20的电子签名的信息(例如,电池交换机120从移动电池20获取的电子证书)的真实性。

[0280] 签名验证公钥84用于解密使用签名私钥82加密的信息。如上所述,通过使用签名私钥82对任意信息进行加密来生成移动电池20的电子签名。此外,电子证书包含任意信息的明文和使用签名私钥82对该任意信息进行加密的密文。签名验证公钥84用于解密使用签名私钥82加密的信息。通过比较包含在电子证书中的明文信息和使用签名验证公钥84解密的信息,可以验证包含在电子证书中的明文信息的真实性。

[0281] 图10概略性地示出了认证公钥74的获取过程的示例。在本实施方式中,电池认证

部378已经从例如密钥发行者50、通信终端52或管理服务器140获取移动电池20的签名验证公钥84。例如,在保存部520中存储对应地存储一个以上的移动电池20的电池ID和一个以上的移动电池20的签名验证公钥84的数据库。注意,多个移动电池20的签名验证公钥84可以相同,并且所有移动电池20的签名验证公钥84也可以相同。

[0282] 在本实施方式中,认证对应部232还包含公钥发送部1012。此外,电池认证部378还包含公钥获取部1014。

[0283] 根据本实施方式,首先,在S1020中,例如,电池交换机120的公钥获取部1014检测移动电池20已经安装在槽124中。当公钥获取部1014检测到移动电池20安装在槽124中时,公钥获取部1014向移动电池20发送激活信号。

[0284] 在S1022中,例如,当移动电池20的公钥发送部1012接收到激活信号时,例如,控制部230和认证对应部232被激活。此时,公钥发送部1012可以向电池交换部120发送表示认证对应部232已经被激活的激活确认信号。

[0285] 接下来,在S1024中,公钥获取部1014向移动电池20发送请求发送电池ID和认证公钥74的信号(有时称为公钥发送请求)。在S1030中,例如,当移动电池20的公钥发送部1012接收到公钥发送请求时,公钥发送部1012使用签名私钥82对认证公钥74进行加密。在S1032中,公钥发送部1012将存储在电池ID保存部252中的电池ID、未加密的认证公钥74和用签名私钥82加密的认证公钥74发送到电池交换机120。

[0286] 使用签名私钥82对认证公钥74进行加密的处理可以是使用签名私钥82对认证公钥74进行签名的处理(有时称为签名处理)的示例。在签名处理中,可以使用各种公钥加密方式或公钥加密基础(PKI)。作为签名处理的方式,例示了RSA密码方式、DSA签名方式、ECDAS签名方式、EdDSA签名方式等。在ECDAS签名方式中,使用了使用椭圆曲线的加密方式。使用公钥密码的公钥将明文变换为密文的过程有时称为加密。使用与加密时使用的公钥配对的私钥将密文变换为明文的过程有时称为解密。用公钥密码的私钥处理明文的过程有时被称为签名。使用公钥密码的公钥将签名变换为原始信息的过程有时称为验证。

[0287] 接下来,在S1040中,当公钥获取部1014从公钥发送部1012接收到电池ID、未加密的认证公钥74和用签名私钥82加密的认证公钥74时,公钥获取部1014参考对应地存储一个以上的移动电池20的电池ID和一个以上的移动电池20的签名验证公钥84的数据库,并提取与由公钥发送部1012发送的电池ID相对应的签名验证公钥84。此外,公钥获取部1014使用提取的签名验证公钥84对由签名私钥82加密的认证公钥74进行解密。注意,在所有移动电池20的签名验证公钥84相同的情况下,可以省略公钥获取部1014参考上述数据库提取签名验证公钥84的步骤。

[0288] 接下来,在S1042中,公钥获取部1014将由公钥发送部1012发送的未加密的认证公钥74与在S1040中解密的认证公钥74进行比较。例如,公钥获取部1014确定由公钥发送部1012发送的未加密的认证公钥74与在S1040中解密的认证公钥74是否匹配。当由公钥发送部1012发送的未加密的认证公钥74与在S1040中解密的认证公钥74匹配时,在S1044中,公钥获取部1014将由公钥发送部1012发送的认证公钥74作为移动电池20的真实认证公钥74存储在保存部520或公钥数据库522中。上述比较处理可以是验证认证公钥74的签名的处理(有时称为验证处理)的示例。

[0289] 认证公钥74可以是第十一信息的示例。签名私钥82可以是第十二信息的示例。使

用签名私钥82加密的认证公钥74可以是第十三信息的示例。签名验证公钥84可以是第十四信息的示例。使用签名验证公钥84解密的认证公钥74可以是第十五信息的示例。签名处理可以是信息的变换的示例。验证处理可以是信息的变换或反向变换的示例。

[0290] 另一实施方式的示例

[0291] 在本实施方式中,以移动电池20安装在电池交换机120上的情况为例,详细描述了电池交换机120获取移动电池20的认证公钥74的过程。然而,获取移动电池20的认证公钥74的主体不限于电池交换机120。在另一实施方式中,获取移动电池20的认证公钥74的主体可以是上述电力装置。

[0292] 此外,如上所述,确认装置不限于电池交换机120。任意确认装置可以通过与本实施方式相同的过程获取任意待确认装置的认证公钥。例如,在移动电池20认证电池交换机120的情况下,移动电池20通过与本实施方式相同的过程获取电池交换机120的认证公钥。

[0293] 在本实施方式中,以在S1030中使用签名私钥82对认证公钥74进行加密,在S1032中,将存储在电池ID保存部252中的电池ID、未加密的认证公钥74和用签名私钥82加密的认证公钥74从移动电池20发送到电池交换机120为例,详细描述了电池交换机120获取移动电池20的认证公钥74的过程。然而,电池交换机120获取移动电池20的认证公钥74的过程不限于本实施方式。例如,在S1030中,使用签名私钥82加密的信息不限于认证公钥74。

[0294] 根据另一实施方式,在S1030中,使用签名私钥82对任意码进行加密。上述码可以具有与上述认证码相同的配置。上述码可以是电池ID。在这种情况下,例如,在S1032中,将存储在电池ID保存部252中的电池ID、未加密的认证公钥74、未加密的上述码和用签名私钥82加密的上述码从移动电池20发送到电池交换机120。

[0295] 接下来,在S1040中,公钥获取部1014提取与由公钥发送部1012发送的电池ID相对应的签名验证公钥84,并使用提取的签名验证公钥84对由签名私钥82加密的码进行解密。此外,在S1042中,公钥获取部1014将由公钥发送部1012发送的未加密码与在S1040中解密的码进行比较。例如,公钥获取部1014判定由公钥发送部1012发送的未加密的码与在S1040中解密的码是否匹配。当两者匹配时,公钥获取部1014将由公钥发送部1012发送的认证公钥74作为移动电池20的真实认证公钥74存储在保存部520或公钥数据库522中。根据上述实施方式,与本实施方式一样,电池交换机120可以确认从电池20接收的认证公钥74是正规的认证公钥。

[0296] 根据又一实施方式,在S1030中,使用签名私钥82对上述任意码的哈希值进行加密。然后,在S1032中,将存储在电池ID保存部252中的电池ID、未加密的认证公钥74、未加密的上述码的哈希值和用签名私钥82加密的上述码的哈希值从移动电池20发送到电池交换机120。在这种情况下,与上述其他实施方式的不同之处在于,在S1042中,公钥获取部1014导出在S1040中解密的码的哈希值。此外,与上述其他实施方式的不同之处在于,公钥获取部1014将由公钥发送部1012发送的未加密的码的哈希值与在S1040中解密的码的哈希值进行比较。

[0297] 根据又一实施方式,使用任意的电子签名方式或电子证书方式将移动电池20的认证公钥74从移动电池20发送到电池交换机120。由此,电池交换机120可以确认从移动电池20接收的认证公钥74是正规的认证公钥。

[0298] 如上所述,在本实施方式中,在S1030中,使用签名私钥82对认证公钥74进行加密。

在S1032中,以存储在电池ID保存部252中的电池ID、未加密的认证公钥74和用签名私钥82加密的认证公钥74从移动电池20发送到电池交换机120的情况为例,详细描述了电池交换机120获取移动电池20的认证公钥74的过程。然而,电池交换机120获取移动电池20的认证公钥74的过程不限于本实施方式。

[0299] 在另一实施方式中,移动电池20的保存部250存储认证公钥74的电子证书。认证公钥74的电子证书包含例如未加密的认证公钥74和用签名私钥82加密的认证公钥74。认证公钥74的电子证书包含例如未加密的电池ID和认证公钥74、以及用签名私钥82加密的电池ID和认证公钥74。当电池交换机120的公钥获取部1014请求发送公钥时,移动电池20的公钥发送部1012向公钥获取部1014发送认证公钥74的电子证书。由此,省略了移动电池20使用签名私钥82对认证公钥74进行加密的处理。在这种情况下,移动电池20可以不存储签名私钥82。

[0300] 在本实施方式中,以公钥获取部1014通过参考对应地存储一个以上的移动电池20的签名验证公钥84的数据库来提取与由公钥发送部1012发送的电池ID相对应的签名验证公钥84的情况为例,详细描述了电池交换部120获取移动电池20的认证公钥74的过程。然而,电池交换机120获取移动电池20的认证公钥74的过程不限于本实施方式。

[0301] 在另一实施方式中,移动电池20的保存部250存储签名验证公钥84的电子证书。签名验证公钥84的电子证书包含例如未加密的签名验证公钥84和用认证机构的私钥加密的签名验证公钥84。签名验证公钥84的电子证书包含例如未加密的ID和签名验证公钥84、以及用签名私钥82加密的ID和签名验证公钥84。上述ID可以是电池ID、移动电池20的制造商的ID、移动电池20的控制CPU或安全IC的制造商的ID。当电池交换机120的公钥获取部1014请求发送公钥时,移动电池20的公钥发送部1012向公钥获取部1014发送签名验证公钥84的电子证书。公钥发送部1012获取与私钥相对应的公钥。与认证机构的私钥相对应的公钥可以存储在电池交换机120中,也可以响应于来自电池交换机120的请求从认证机构的服务器发送到电池交换机120。

[0302] 图11概略性地示出了认证公钥74的获取过程的示例。根据本实施方式,认证公钥74的获取过程与参考图10描述的不同之处在于,在执行S1030之后执行S1132而不是S1032,以及在执行S1132之后执行S1134。关于上述差异以外的特征,参考图11描述的认证公钥74的获取过程可以具有与参考图10描述的认证公钥74的获取过程相同的配置。

[0303] 根据本实施方式,在S1132中,公钥发送部1012将存储在电池ID保存部252中的电池ID、未加密的认证公钥74、用签名私钥82加密的认证公钥74和签名验证公钥84发送到电池交换机120。公钥发送部1012可以向电池交换机120发送包含签名验证公钥84的电子证书,从而向电池交换机120发送签名验证公钥84。

[0304] 如上所述,公钥发送部1012可以响应于来自公钥获取部1014的请求,将存储在电池ID保存部252中的电池ID、认证公钥74的电子证书和签名验证公钥84的电子证书发送到电池交换机120。公钥获取部1014可以代替公钥请求或与公钥请求一起请求发送电子证书。如上所述,认证公钥74的电子证书包含例如未加密的电池ID和认证公钥74、以及用签名私钥82加密的电池ID和认证公钥74。在这种情况下,公钥发送部1012可以响应于来自公钥获取部1014的请求,向电池交换部120发送认证公钥74的电子证书和签名验证公钥84的电子证书。

[0305] 在S1134中,公钥获取部1014请求可信认证机构(未示出)确认签名验证公钥84的有效性或真实性。当确认了签名验证公钥84的有效性或真实性时,公钥获取部1014执行S1040、S1042和S1044。签名验证公钥84例如由参考图4描述的控制CPU或安全IC的制造商或销售商发行。因此,根据另一实施方式,公钥获取部1014可以例如从控制CPU或安全IC的制造商或销售商获取签名验证公钥84。

[0306] 上述可信认证机构可以是管理服务器140,或者可以是不同于管理服务器140的服务器。上述可信认证机构可以是由控制CPU或安全IC的制造商或销售商管理或操作的服务器。签名验证公钥84可以具有有效期。上述可信认证机构可以管理签名验证公钥84的有效期。例如,当认证机构从公钥发送部1012接收到关于确认签名验证公钥84的有效性或真实性的请求时,认证机构可以判定签名验证公钥84的有效期是否已过期。当签名验证用公钥84的有效期过期时,认证机构响应于上述请求,向公钥发送部1012发送表示签名验证用公钥84无效的信息。另一方面,如果签名验证公钥84没有过期,则认证机构响应于上述请求,将表示签名验证用公钥84有效的信息发送到公钥发送部1012。

[0307] 另一实施方式的示例

[0308] 在本实施方式中,以移动电池20安装在电池交换机120上的情况为例,详细描述了电池交换机120获取移动电池20的认证公钥74的过程。然而,获取移动电池20的认证公钥74的主体不限于电池交换机120。在另一实施方式中,获取移动电池20的认证公钥74的主体可以是上述电力装置。

[0309] 此外,如上所述,确认装置不限于电池交换机120。任意确认装置可以通过与本实施方式相同的过程获取任意待确认装置的认证公钥。例如,在移动电池20认证电池交换机120的情况下,移动电池20通过与本实施方式相同的过程获取电池交换机120的认证公钥。

[0310] 在本实施方式中,在S1030中,使用签名私钥82对认证公钥74进行加密。在S1132中,以存储在电池ID保存部252中的电池ID、未加密的认证公钥74、用签名私钥82加密的认证公钥74和签名验证公钥84从移动电池20发送到电池交换机120的情况为例,详细描述了电池交换机120获取移动电池20的认证公钥74的过程。然而,电池交换机120获取移动电池20的认证公钥74的过程不限于本实施方式。例如,在S1030中,使用签名私钥82加密的信息不限于认证公钥74。

[0311] 根据另一实施方式,在S1030中,使用签名私钥82对任意码进行加密。上述码可以具有与上述认证码相同的配置。上述码可以是电池ID。在这种情况下,例如,在S1032中,将存储在电池ID保存部252中的电池ID、未加密的认证公钥74、未加密的上述码、用签名私钥82加密的上述码和签名验证公钥84从移动电池20发送到电池交换机120。

[0312] 接下来,在S1040中,公钥获取部1014使用在S1134中确认了有效性或真实性的签名验证公钥84,对由签名私钥82加密的码进行解密。此外,在S1042中,公钥获取部1014将由公钥发送部1012发送的未加密的码与在S1040中解密的码进行比较。例如,公钥获取部1014确定由公钥发送部1012发送的未加密的码与在S1040中解密的码是否匹配。当两者匹配时,公钥获取部1014将由公钥发送部1012发送的认证公钥74作为移动电池20的真实认证公钥74存储在保存部520或公钥数据库522中。根据上述实施方式,与本实施方式一样,电池交换机120可以确认从移动电池20接收的认证公钥74是正规的认证公钥。

[0313] 根据又一实施方式,在S1030中,使用签名私钥82对上述任意码的哈希值进行加

密。然后,执行与结合图10的另一实施方式描述的过程类似的过程。

[0314] 根据又一实施方式,使用任意的电子签名方式或任意的电子认证方式将移动电池20的认证公钥74从移动电池20发送到电池交换机120。由此,电池交换机120可以确认从移动电池20接收的认证公钥74是正规的认证公钥。

[0315] 在结合图11描述的实施方式中,也可以进行与结合图10描述的另一实施方式相同的改变。例如,在另一实施方式中,移动电池20的保存部250可以存储认证公钥74的电子证书。当电池交换机120的公钥获取部1014请求发送公钥时,移动电池20的公钥发送部1012可以将存储在保存部250中的电子证书发送到公钥获取部1014,而不用新创建认证公钥74的电子证书。由此,省略了移动电池20使用签名私钥82对认证公钥74进行加密的处理。在这种情况下,移动电池20可以不存储签名私钥82。在下面描述的任何实施方式中,可以进行类似的改变。

[0316] 将参考图12、图13、图14和图15描述移动电池20的认证过程的另一示例。图12概略性地示出了移动电池20的认证过程的另一示例。图13概略性地示出了响应码和验证码之间的关系的示例。图14概略性地示出了响应码和验证码的验证过程的示例。图15概略性地示出了响应码和验证码的验证过程的另一示例。

[0317] 结合图12描述的认证过程与结合图4描述的认证过程的不同之处在于,明文的认证码作为质询码被发送。与参考图4描述的认证过程相同或相似的过程被赋予与图4相同的附图标记,并且有时省略对该过程的描述。与参考图4描述的认证过程相同或相似的过程可以具有与参考图4描述的认证过程相同的配置。

[0318] 在本实施方式中,以电池交换机120认证移动电池20的情况为示例,描述用于确认装置确认待确认装置是否是合法装置的信息处理的示例。然而,上述信息处理不限于本实施方式。在另一实施方式中,移动电池20可以通过与本实施方式相同的过程来认证电池交换机120。

[0319] 如图12所示,根据本实施方式,当电池认证部378在S3130中获取移动电池20的电池ID时,在S3130中,电池认证部378使用电池ID作为关键字来参考与上述认证公钥74相关的数据库,提取与电池ID匹配的认证公钥74。当没有提取到与电池ID匹配的认证公钥74时,电池认证部378可以访问通信终端52或管理服务器140,以获取与电池ID匹配的认证公钥74。

[0320] 此外,当电池认证部378在S3130中获取了移动电池20的电池ID时,在S3130中,电池认证部378生成质询码,并将质询码发送到移动电池20。例如,通过以下过程执行质询码的生成和发送。

[0321] 电池认证部378首先准备认证码。例如,电池认证部378生成随机数,并确定使用该随机数作为认证码。电池认证部378可以使用上述随机数生成认证码。电池认证部378可以基于上述随机数和公钥加密方式中使用的任何参数来生成认证码。在公钥加密方式中使用的参数在确认装置和待确认装置之间共享,例示有公共参数。公共参数的示例包含椭圆曲线密码的椭圆曲线E、该椭圆曲线E的生成源P等。

[0322] 电池认证部378将上述认证码作为质询码发送到移动电池20。电池认证部378将未由认证公钥74加密的认证码作为质询码发送到移动电池20。例如,电池认证部378将明文的认证码作为质询码发送到移动电池20。

[0323] 在S3132中,电池认证部378使用上述认证码和移动电池20的认证公钥74来生成验证码。在基于随机数和公共参数生成认证码的情况下,电池认证部378可以使用用于生成认证码的随机数和移动电池20的认证公钥74来生成与上述相同的验证码。稍后将详细描述生成验证码的过程。

[0324] 在S3134中,当移动电池20的控制部230接收到质询码时,控制部230使用包含在质询码中的认证码和移动电池20的认证私钥72来生成响应码。稍后将详细描述生成响应码的过程。此外,在S3136中,控制部230将响应码发送到电池交换机120。由此,控制部230结束与电池交换机120的认证处理相对应的处理(有时称为认证对应处理)。

[0325] 在S3138中,当电池认证部378接收到响应码时,电池认证部378验证响应码和验证码是否具有预定的数学关系。上述验证过程的细节将在后面描述。此后,在S440中,电池认证部378基于上述验证结果判定或确认移动电池20是否是合法装置。

[0326] 图13概略性地示出了响应码和验证码之间的关系的示例。在本实施方式中,通过使用待确认装置的认证公钥和认证私钥来生成响应码和验证码。当待确认装置是移动电池20时,使用认证公钥74和认证私钥72生成响应码和验证码。认证私钥72例如存储在保存部250中。即使在待确认装置是电池交换机120的情况下,也可以通过与待确认装置是移动电池20的情况相同的过程来生成响应码和验证码。

[0327] 生成待确认装置的认证公钥和认证私钥以满足数学关系3212。作为数学关系3212,例示了在使用椭圆曲线的加密(有时称为椭圆曲线加密或ECC)中使用的关系。下面的公式1举例说明了上述关系。在公式1中,p、a和b中的每一个是椭圆曲线的参数。

[0328] (公式1)

[0329] $y^2=x^3+a\times+b \bmod p$

[0330] 由公式1表示的椭圆曲线上的点亦即基点G(x,y)通过整数n(有时称为阶数)进行标量倍算得到的点nG(x,y)位于公式1表示的椭圆曲线上。此时,充分大的阶数n被用作私钥,nG(x,y)被用作公钥。

[0331] 当待确认装置是合法装置时,生成响应码和验证码,使得响应码和验证码满足数学关系3214。基于数学关系3212确定数学关系3214。在一个实施方式中,响应码和验证码可以相同。在这种情况下,数学关系3214是响应码=验证码或响应码÷验证码=1。在其他实施方式中,响应码和验证码可以不同。作为上述计算结果的1可以是预定值的示例。

[0332] 在参考图13描述的实施方式中,电池认证部378包含认证码生成部3220、验证码生成部3230和验证部3250。控制部230包含响应码生成部3240。

[0333] 在本实施方式中,认证码生成部3220生成认证码3222。例如,认证码生成部3220使随机数生成器生成随机数,并基于该随机数生成认证码3222。认证码生成部3220可以输出上述随机数作为认证码3222。例如,认证码生成部3220将明文的认证码3222输出到响应码生成部3240和验证码生成部3230。

[0334] 在本实施方式中,验证码生成部3230获取认证码3222。验证码生成部3230获取认证公钥。验证码生成部3230使用认证码3222导出验证码3232。例如,验证码生成部3230基于认证公钥变换验证码3222,并生成验证码3232。验证码生成部3230将验证码3232输出到验证部3250。稍后将详细描述验证码生成部3230。

[0335] 在本实施方式中,响应码生成部3240获取认证码3222。响应码生成部3240获取认

证私钥。响应码生成部3240基于认证码3222和认证私钥生成响应码3242。响应码生成部3240例如基于认证私钥变换认证码3222,并生成响应码3242。

[0336] 响应码生成部3240可以生成与通过基于认证公钥变换认证码3222而获得的信息(即,验证码3232)相同的信息。响应码生成部3240例如基于认证码3222、认证私钥和数学关系3212和/或数学关系3214生成与验证码3232相同的信息。

[0337] 响应码生成部3240将响应码3242输出到验证部3250。稍后将详细描述响应码生成部3240。

[0338] 在本实施方式中,验证部3250从验证码生成部3230获取验证码3232。验证部3250从响应码生成部3240获取响应码3242。验证部3250基于验证码3232和响应码3242来判定待确认装置是否是合法装置。

[0339] 当响应码生成部3240输出通过基于认证私钥变换认证码3222而获得的信息作为响应码3242时,验证部3250可以判定验证码3232和响应码3242是否满足数学关系3214。当响应码生成部3240输出与验证码3232相同的信息作为响应码3242时,验证部3250可以比较验证码3232和响应码3242。稍后将描述验证部3250的细节。

[0340] 数学关系3212可以是第一数学关系的示例。数学关系3214可以是第二数学关系的示例。认证码生成部3220可以是第一验证信息生成部的示例。认证码3222可以是第一验证信息的示例。验证码生成部3230可以是第三验证信息生成部的示例。验证码3232可以是第三验证信息的示例。响应码生成部3240可以是第一验证信息获取部或响应部的示例。响应码3242可以是第五验证信息或第六验证信息的示例。验证部3250可以是响应接收部或确定部的示例。

[0341] 认证码3222的输出可以是第一验证信息的发送的示例。响应码生成部3240获取认证码3222的过程可以是待确认装置从确认装置接收第一验证信息的步骤或从第一电力装置获取第一验证信息的步骤的示例。响应码生成部3240将响应码3242输出到验证部3250的过程可以是待确认装置基于第一验证信息和第四验证信息生成第五验证信息的步骤的示例。用于生成验证码3232的公钥可以是第二验证信息的示例。用于生成响应码3242的私钥可以是第四验证信息的示例。

[0342] 图14概略性地示出了响应码和验证码的验证过程的示例。在本实施方式中,为了便于理解本实施方式,将以待确认装置是移动电池20的情况为例详细描述响应码和验证码的验证过程。熟悉本申请说明书的本领域技术人员可以理解,例如,即使在被确认的装置是电池交换机120的情况下,也可以通过与本实施方式相同的过程来验证响应码和验证码。在本实施方式中,以响应码生成部3240输出通过基于认证私钥变换认证码3222而获得的信息作为响应码3242的情况为例,详细描述响应码和验证码的验证过程。

[0343] 在本实施方式中,验证码生成部3230例如包含第一运算部3310。响应码生成部3240例如包含第一运算部3310、第二运算部3320和第三运算部3330。验证部3250例如包含第三运算部3330和判定部3350。

[0344] 在本实施方式中,第一运算部3310获取认证码3222和认证公钥74。例如,第一运算部3310基于认证公钥74变换认证码3222,并生成验证码3232。第一运算部3310可以通过使用认证公钥74对认证码3222进行加密来生成验证码3232。第一运算部3310将验证码3232输出到第三运算部3330。

[0345] 在本实施方式中,第二运算部3320获取认证码3222和认证私钥72。例如,第二运算部3320基于认证私钥72变换认证码3222,并生成响应码3242。第一运算部3310可以通过使用认证私钥72对认证码3222进行加密来生成响应码3242。第二运算部3320将响应码3242输出到第三运算部3330。

[0346] 在本实施方式中,第三运算部3330获取验证码3232和响应码3242。第三运算部3330根据第一验证算法对验证码3232和响应码3242进行信息处理,并输出信息处理的运算结果。第一验证算法可以是用于验证验证码3232和响应码3242是否满足数学关系3214的算法。第一验证算法可以包含导出上述椭圆曲线的参数p的过程。第一验证算法可以包含当输入验证码3232和响应码3242并且待确认装置是合法装置时输出根据数学关系3214确定的值的过程。

[0347] 响应码生成部3240的第三运算部3330根据第一验证算法对由响应码生成部3240的第一运算部3310输出的验证码3232和由响应码生成部3240的第二运算部3320输出的响应码3242执行信息处理。响应码生成部3240的第三运算部3330将运算结果3332输出到判定部3350。

[0348] 在移动电池20是合法装置的情况下,运算结果3332表示在认证私钥72和认证公钥74满足数学关系3212的情况下,根据第一验证算法对验证码3232和响应码3242进行信息处理时可以获得的运算结果。如上所述,当待确认装置是合法装置时,验证码3232和响应码3242满足数学关系3212。

[0349] 验证部3250的第三运算部3330根据第一验证算法对由验证码生成部3230的第一运算部3310输出的验证码3232和由响应码生成部3240的第二运算部3320输出的响应码3242执行信息处理。验证部3250的第三运算部3330将运算结果输出到判定部3350。

[0350] 在本实施方式中,判定部3350判定由验证码生成部3230输出的验证码3232和由响应码生成部3240输出的响应码3242是否满足数学关系3214。例如,判定部3350将响应码生成部3240的第三运算部3330的运算结果3332与验证部3250的第三运算部3330的运算结果进行比较。判定部3350可以判定响应码生成部3240的第三运算部3330的运算结果3332是否与验证部3250的第三运算部3330的运算结果匹配。判定部3350可以基于比较结果来确定移动电池20是否正规。

[0351] 当两者匹配时,判定部3350可以判定由验证码生成部3230输出的验证码3232和由响应码生成部3240输出的响应码3242满足数学关系3214。在这种情况下,判定部3350可以确定移动电池20是正规的。当两者不匹配时,判定部3350可以判定由验证码生成部3230输出的验证码3232和由响应码生成部3240输出的响应码3242不满足数学关系3214。在这种情况下,判定部3350可以确定移动电池20不正规或移动电池20非正规。

[0352] 表示响应码生成部3240的第三运算部3330的运算结果的信息可以是第八验证信息的示例。表示验证部3250的第三运算部3330的运算结果的信息可以是第七验证信息的示例。

[0353] 图15概略性地示出了响应码和验证码的验证过程的另一示例。在本实施方式中,为了便于理解本实施方式,将以待确认装置是移动电池20的情况为例详细描述响应码和验证码的验证过程。熟悉本申请说明书的本领域技术人员可以理解,例如,即使在待确认装置是电池交换机120的情况下,也可以通过与本实施方式相同的过程来验证响应码和验证码。

在本实施方式中,以响应码生成部3240输出与验证码3232相同的信息作为响应码3242的情况为例,详细描述响应码和验证码的验证过程。

[0354] 在本实施方式中,验证码生成部3230例如包含第一运算部3310。响应码生成部3240例如包含第四运算部3440。验证部3250例如包含判定部3350。

[0355] 在本实施方式中,第四运算部3440根据认证码3222和认证私钥72导出与验证码3232相同的信息。响应码生成部3240可以将与验证码3232相同的信息作为响应码3242输出到判定部3350。

[0356] 例如,第四运算部3440基于认证码3222、认证私钥72和数学关系3212和/或数学关系3214生成与验证码3232相同的信息。第四运算部3440可以使用数学关系3214,根据认证码3222和认证私钥72生成与验证码3232相同的信息。第四运算部3440可以使用数学关系3214,根据通过基于认证私钥72变换认证码3222而获得的信息生成与验证码3232相同的信息。

[0357] 第四运算部3440可以包含与参考图14描述的响应码生成部3240相同的配置。第四运算部3440可以基于从第二运算部3320输出的响应码3242和从第三运算部3330输出的运算结果3332来生成与验证码3232相同的信息。

[0358] 在本实施方式中,判定部3350将由验证码生成部3230输出的验证码3232与由响应码生成部3240输出的响应码3242进行比较。例如,判定部3350判定由验证码生成部3230输出的验证码3232和由响应码生成部3240输出的响应码3242是否匹配。判定部3350可以基于比较结果来确定移动电池20是否正规。

[0359] 当两者匹配时,判定部3350可以确定移动电池20是正规的。当两者不匹配时,判定部3350可以确定移动电池20不正规或移动电池20非正规。

[0360] 图16示出可以整体地或部分地实现本发明的多个实施方式的计算机5000的示例。电池管理系统100的至少一部分可以由计算机5000实现。例如,控制部230或其一部分可以由计算机5000实现。例如,控制部336或其一部分可以由计算机5000实现。例如,控制部376或其一部分可以由计算机5000实现。

[0361] 安装于计算机5000的程序能够使计算机5000作为本发明的实施方式涉及的装置相关联的操作或该装置的一个或多个“单元”发挥功能,或能够使计算机5000执行该操作或该一个或多个“单元”,以及/或能够使计算机5000执行本发明的实施方式涉及的处理或该处理的步骤。这样的程序为了使计算机5000执行与本说明书所述的流程图以及框图的功能块中的某些或全部相关联的特定的操作而可以被CPU5012执行。

[0362] 本实施方式的计算机5000包括CPU5012、RAM5014、GPU5016以及显示器设备5018,它们通过主控制器5010相互连接。计算机5000还包括通信接口5022、硬盘驱动器5024、DVD-ROM驱动器5026以及IC卡驱动器这样的输入输出单元,它们经由输入输出控制器5020与主控制器5010连接。计算机还包括ROM5030以及键盘5042这样的传统的输入输出单元,它们经由输入输出芯片5040与输入输出控制器5020连接。

[0363] CPU5012按照ROM5050以及RAM5014内保存的程序工作,由此控制各单元。GPU5016在RAM5014内所提供的帧缓冲器等或其自身中获取由CPU5012生成的图像数据,并使图像数据在显示器设备5018上显示。

[0364] 通信接口5022经由网络与其他的电子设备通信。硬盘驱动器5024保存由计算机

5000内的CPU5012使用的程序以及数据。DVD-ROM驱动器5026将程序或数据从DVD—ROM5001等读取,并经由RAM5014将程序或数据向硬盘驱动器5024提供。IC卡驱动器从IC卡读取程序以及数据,以及/或将程序以及数据写入IC卡。

[0365] ROM5030在其内部保存被激活时由计算机5000执行的启动程序等、以及/或依赖于计算机5000的硬件的程序。输入输出芯片5040还可以经由并行端口、串行端口、键盘端口、鼠标端口等,将各种输入输出单元与输入输出控制器5020连接。

[0366] 程序由DVD—ROM5001或IC卡那样的计算机可读存储介质提供。程序被从计算机可读存储介质读取,安装至也是计算机可读存储介质的例子的硬盘驱动器5024、RAM5014或ROM5030,并由CPU5012执行。这些程序内记载的信息处理被计算机5000读取,实现程序和上述各种类型的硬件资源之间的协作。装置或方法可以通过遵从计算机5000的使用而实现信息的操作或处理来构成。

[0367] 例如,在计算机5000和外部设备之间执行通信的情况下,CPU5012可以执行加载到RAM5014的通信程序,基于通信程序中记述的处理,对通信接口5022指示通信处理。通信接口5022在CPU5012的控制下,对向RAM5014、硬盘驱动器5024、DVD—ROM5001或IC卡那样的存储介质内提供的发送缓冲处理区域中保存的发送数据进行读取,将读取的发送数据向网络发送,或将从网络接收的接收数据写入至向存储介质上提供的接收缓冲处理区域等。

[0368] 另外,CPU5012可以使得硬盘驱动器5024、DVD-ROM驱动器5026(DVD—ROM5001)、IC卡等那样的外部存储介质中保存的文件或数据库的全部或所需的部分被读取至RAM5014,并对RAM5014上的数据执行各种类型的处理。CPU5012可以接着将被处理的数据写回至外部存储介质。

[0369] 可以将各种类型的程序、数据、表格以及数据库那样的各种信息保存至存储介质,并受理信息处理。CPU5012可以对从RAM5014读取的数据执行本公开各处记载的、包含由程序的指令序列指定的各种操作、信息处理、条件判断、条件分支、无条件分支、信息的检索/置换等的各种处理,并将结果写回至RAM5014。另外,CPU5012可以检索存储介质内的文件、数据库等中的信息。例如,在分别具有与第2属性的属性值建立了关联的第1属性的属性值的多个项目被保存在存储介质内的情况下,CPU5012可以从该多个项目中检索指定了第1属性的属性值的与条件一致的项目,读取该项目内保存的第2属性的属性值,由此获取与满足预先设定的条件的第1属性建立了关联的第2属性的属性值。

[0370] 以上说明的程序或软件模块可以保存至计算机5000上或计算机5000附近的计算机可读存储介质中。另外,向与专用通信网络或互联网连接的服务器系统内提供的硬盘或RAM那样的存储介质可以作为计算机可读存储介质来使用,由此将上述程序经由网络提供给计算机5000。

[0371] 以上,利用实施方式对本发明进行了说明,但本发明的技术范围不限于上述实施方式所记载的范围。能够对上述实施方式进行多种变更或改良对于本领域技术人员而言是显而易见的。另外,在技术上不矛盾的范围内,可以将针对特定的实施方式说明的事项应用于其他的实施方式。另外,各构成要素可以具有名称相同而参照符号不同的其他构成要素相同的特征。进行了这样的变更或改良的方式也能够包含于本发明的技术范围内从权利要求书的记载而言是显而易见的。

[0372] 对于权利要求书、说明书以及附图中示出的装置、系统、程序以及方法中的动作、

流程、步骤以及阶段等的各处理的执行顺序而言，应注意没有特别明示“之前”、“先行”等，另外，只要不是将之前的处理的输出在之后的处理中使用，就可以以任意的顺序实现。对于权利要求书、说明书以及附图中的动作流程而言，即使为了便利而使用了“首先”、“接着”等进行了说明，但并不意味着必须以这样的顺序来实施。

[0373] 附图标记说明

[0374] 12电力系统、14通信网络、20移动电池、30电动自行车、40用户、42通信终端、50密钥发行者、52通信终端、72认证私钥、74认证公钥、82签名私钥、84签名验证公钥、100电池管理系统、120电池交换机、122保管单元、124槽、126通信单元、128通信接口、140管理服务器、212电力连接器、214通信连接器、220蓄电部、230控制部、232认证对应部、240感测部、250保存部、252电池ID保存部、254认证私钥保存部、310通信线路、312不间断电源装置、314路由器、320壳体、330搭载设备、332感测部、334设定保存部、336控制部、360壳体、370搭载设备、372用户接口、374用户识别部、376控制部、378电池认证部、502认证码、504哈希值、506哈希值、512质询码、516响应码、520保存部、522公钥数据库、524白名单、530电池ID获取部、540认证码生成部、550验证码生成部、552哈希函数、560质询码生成部、562质询码发送部、570响应码获取部、582比较部、584判定部、620请求接收部、630ID发送部、640质询码获取部、650质询码解密部、660响应码生成部、662哈希函数、670响应码发送部、710断路器、712电力线、714AC/DC电源、716分配器、718电力线、730主控板、732通信集线器、734通信线路、742温度调节部、744蜂鸣器、746感测部、748维护门、760AC/DC充电器、762电力连接器、770槽控制板、772通信连接器、774驱动部、776闸门、778锁定部、782温度调节部、784状态显示部、786感测部、814AC/DC电源、816服务插座、820CPU板、830以太网接口、842NFC读取器、844照相机、852触摸面板、854显示器、856扬声器、920移动电池、955认证公钥保存部、956签名私钥保存部、957签名验证公钥保存部、1012公钥发送部、1014公钥获取部、3212数学关系、3214数学关系、3220认证码生成部、3222认证码、3230验证码生成部、3232验证码、3240响应码生成部、3242响应码、3250验证部、3310第一运算部、3320第二运算部、3330第三运算部、3332运算结果、3350判定部、3440第四运算部、5000计算机、5001DVD－ROM、5010主控制器、5012CPU、5014RAM、5016GPU、5018显示器设备、5020输入输出控制器、5022通信接口、5024硬盘驱动器、5026DVD－ROM驱动器、5030ROM、5040输入输出芯片、5042键盘。

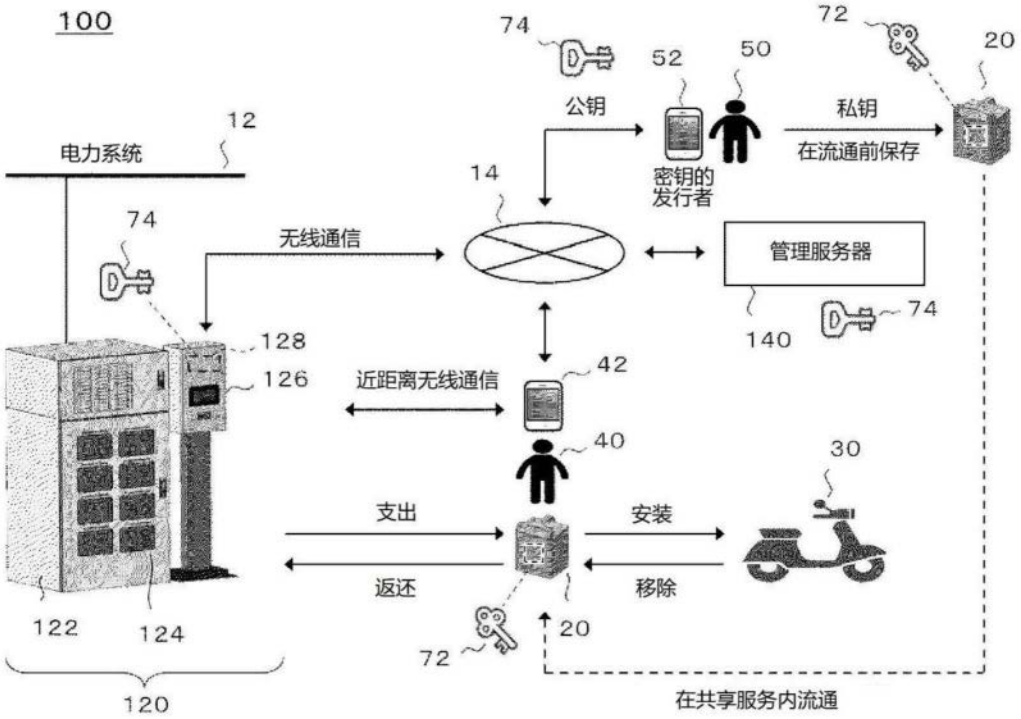

100
74
72
20
52
50
公钥
私钥
在流通前保存
12
电力系统
14
密钥的
发行者
74
无线通信
管理服务器
140
74
128
126
近距离无线通信
42
40
30
支出
安装
返还
移除
122
124
72
20
120
在共享服务内流通

图1

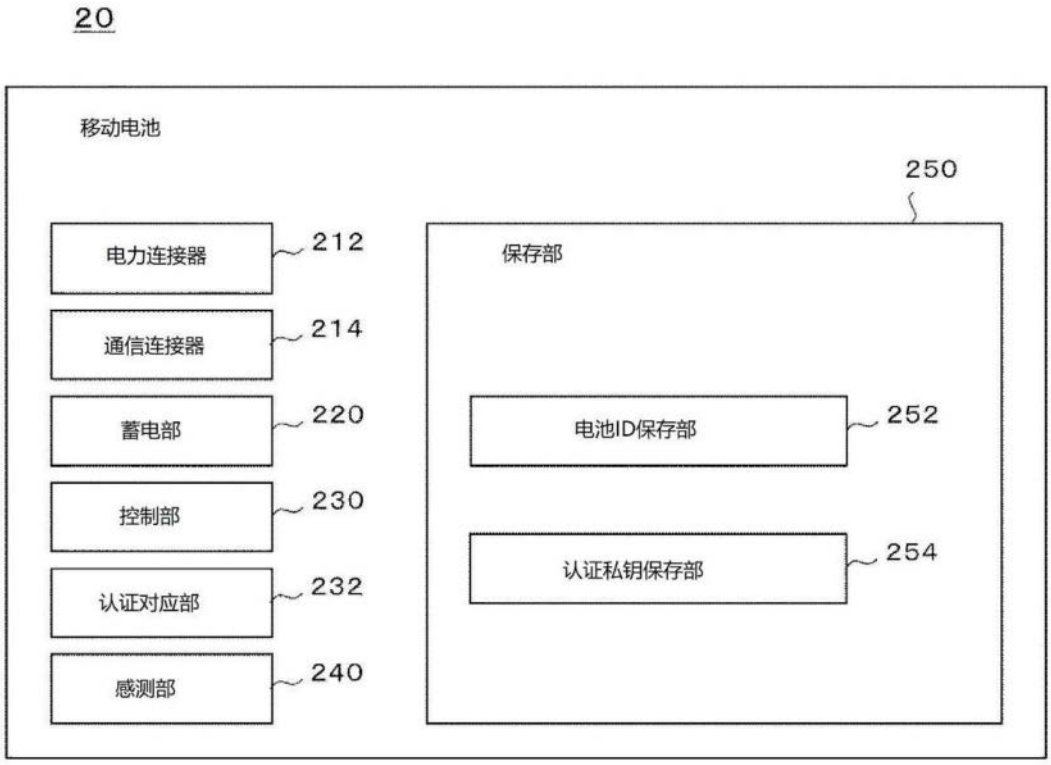

20
移动电池
250
电力连接器
212
保存部
通信连接器
214
蓄电部
220
电池ID保存部
252
控制部
230
认证私钥保存部
254
认证对应部
232
感测部
240

图2

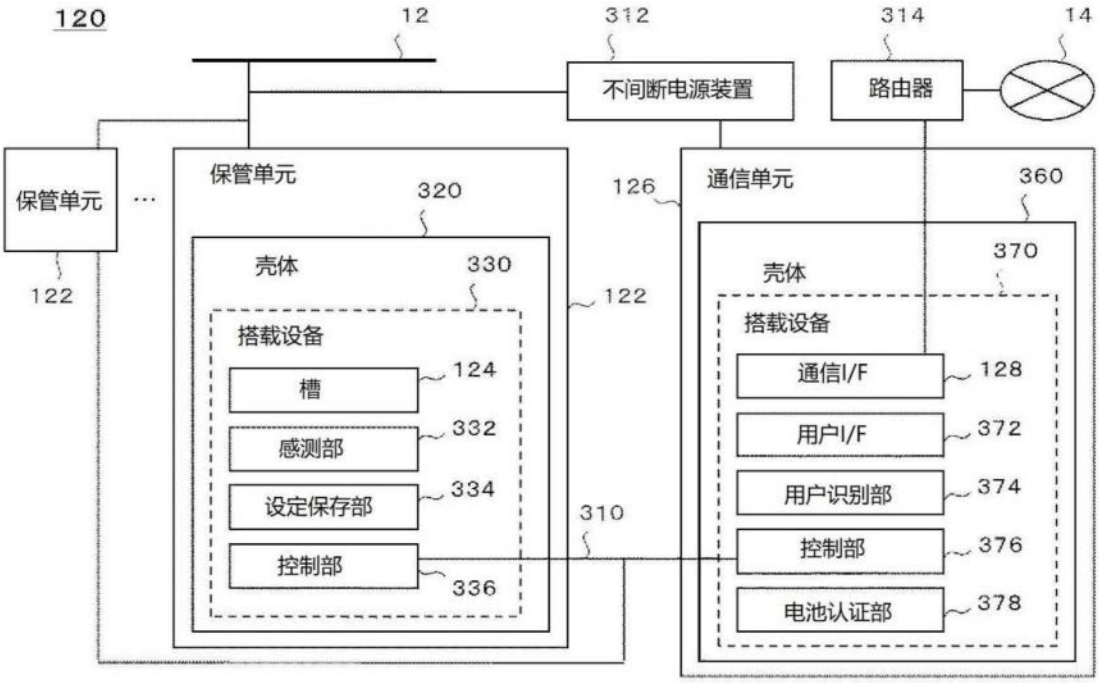

120
12
312
314
14
不间断电源装置
路由器
保管单元
保管单元
320
126
通信单元
360
122
壳体
330
122
壳体
370
搭载设备
搭载设备
槽
124
通信I/F
128
感测部
332
用户I/F
372
设定保存部
334
用户识别部
374
310
控制部
336
控制部
376
电池认证部
378

图3

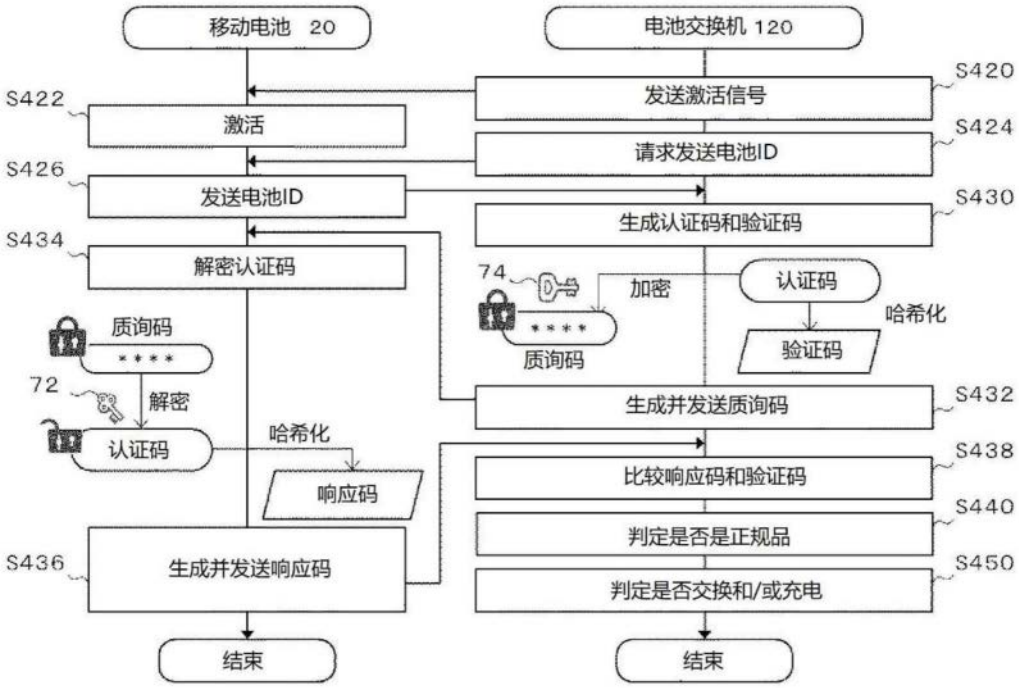

移动电池 20
电池交换机 120
S420
发送激活信号
S422
激活
S424
请求发送电池ID
S426
发送电池ID
S430
生成认证码和验证码
S434
解密认证码
74
加密
认证码
哈希化
质询码
质询码
验证码
72
解密
S432
生成并发送质询码
认证码
哈希化
S438
比较响应码和验证码
响应码
S440
判定是否是正规品
S436
生成并发送响应码
S450
判定是否交换和/或充电
结束
结束

图4

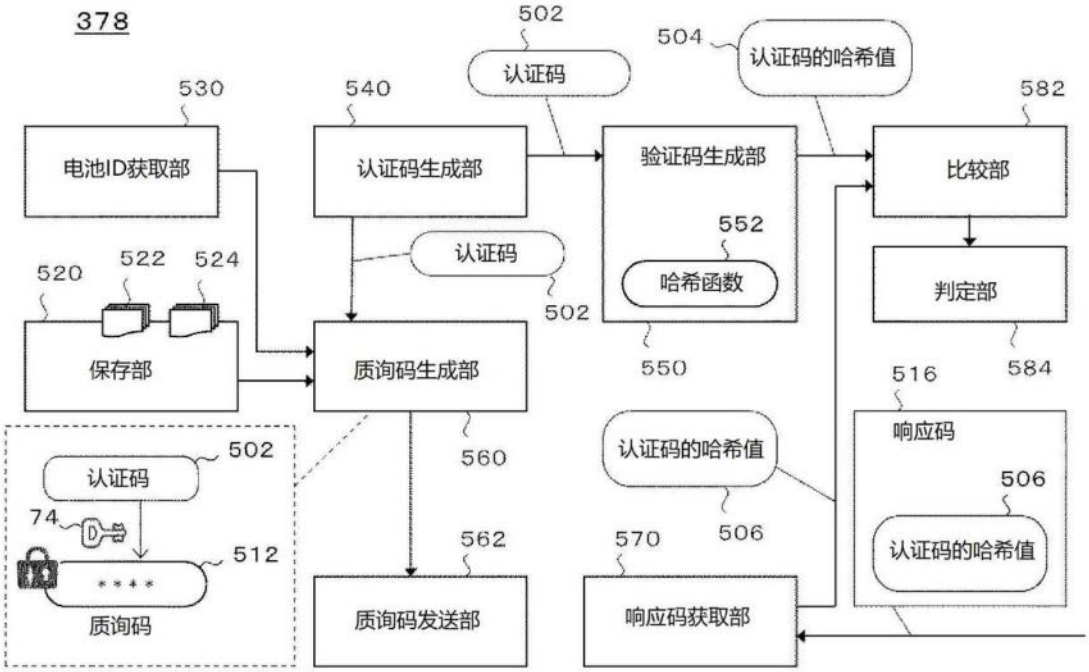

378
502
认证码
504
认证码的哈希值
530
540
582
电池ID获取部
认证码生成部
验证码生成部
比较部
552
哈希函数
认证码
502
520
522
524
保存部
质询码生成部
550
判定部
584
516
560
认证码的哈希值
响应码
506
502
认证码
74
512
562
570
506
认证码的哈希值
质询码
质询码发送部
响应码获取部

图5

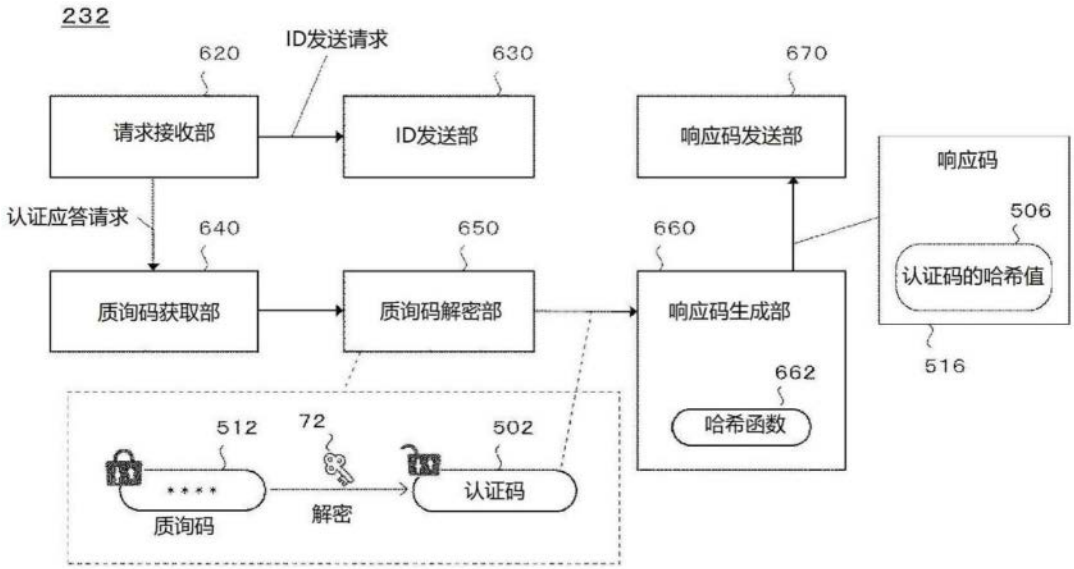

232
ID发送请求
620
630
670
请求接收部
ID发送部
响应码发送部
响应码
506
认证应答请求
640
650
660
认证码的哈希值
质询码获取部
质询码解密部
响应码生成部
516
662
哈希函数
512
72
502
认证码
质询码
解密

图6

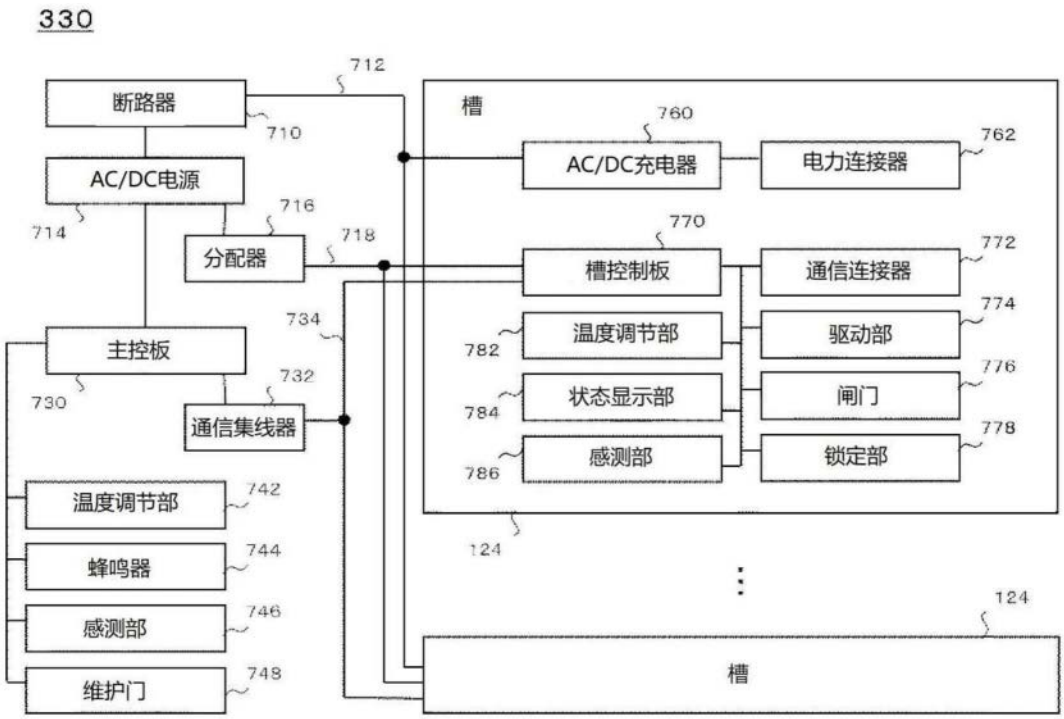

330
712
断路器
710
AC/DC电源
714
716
分配器
718
734
主控板
730
732
通信集线器
温度调节部
742
蜂鸣器
744
感测部
746
维护门
748
槽
760
AC/DC充电器
762
电力连接器
770
槽控制板
772
通信连接器
782
温度调节部
774
驱动部
784
状态显示部
776
闸门
786
感测部
778
锁定部
124
124
槽

图7

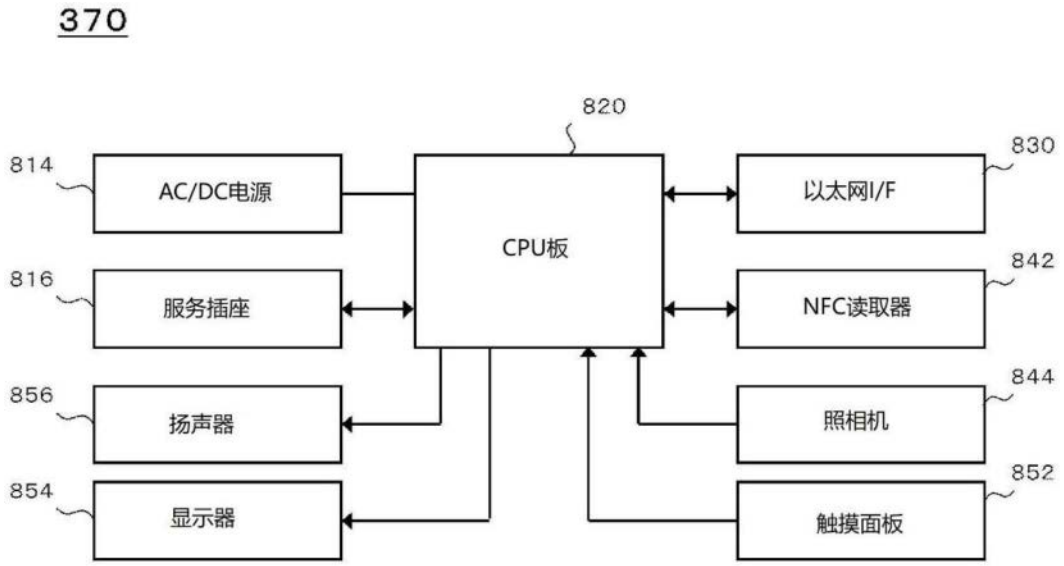

370
820
814
AC/DC电源
CPU板
830
以太网I/F
816
服务插座
842
NFC读取器
856
扬声器
844
照相机
854
显示器
852
触摸面板

图8

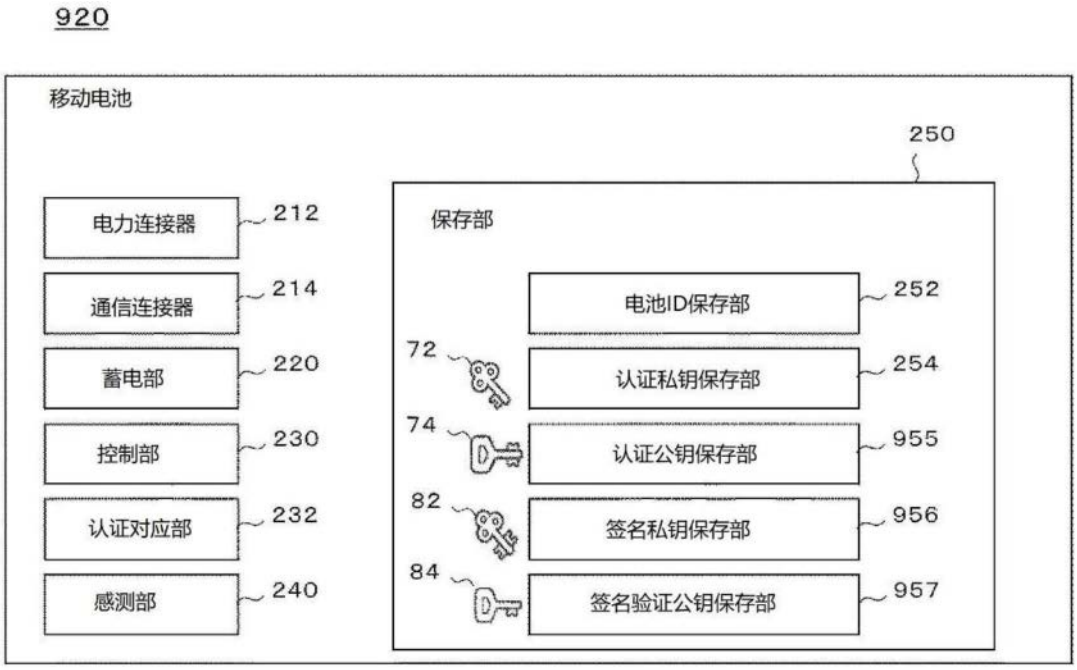

920
移动电池
250
电力连接器
212
通信连接器
214
蓄电部
220
控制部
230
认证对应部
232
感测部
240
保存部
电池ID保存部
252
72
认证私钥保存部
254
74
认证公钥保存部
955
82
签名私钥保存部
956
84
签名验证公钥保存部
957

图9

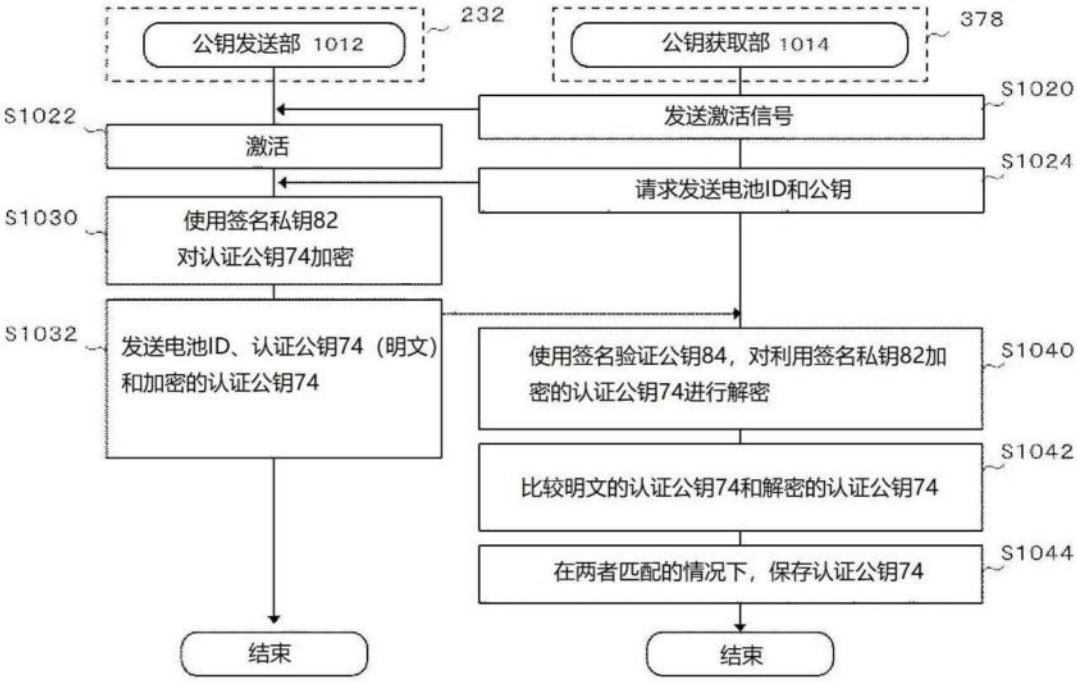

232
公钥发送部 1012
378
公钥获取部 1014
S1020
发送激活信号
S1022
激活
S1024
请求发送电池ID和公钥
S1030
使用签名私钥82
对认证公钥74加密
S1032
发送电池ID、认证公钥74（明文）
和加密的认证公钥74
S1040
使用签名验证公钥84，对利用签名私钥82加密的认证公钥74进行解密
S1042
比较明文的认证公钥74和解密的认证公钥74
S1044
在两者匹配的情况下，保存认证公钥74
结束
结束

图10

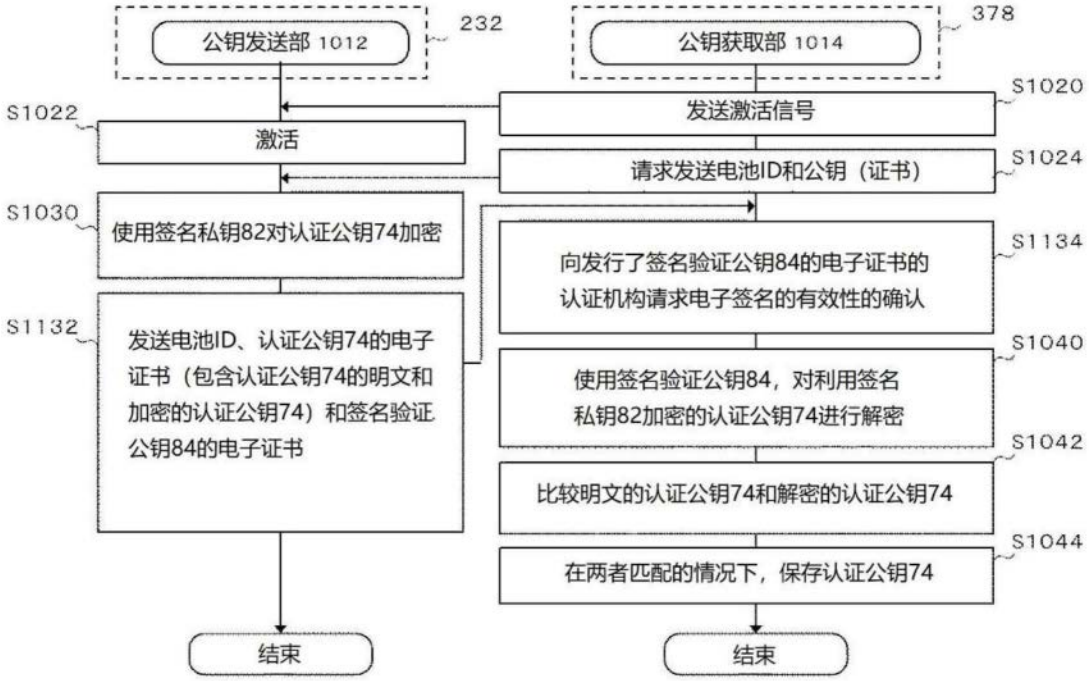

公钥发送部 1012
232
公钥获取部 1014
378
S1020
发送激活信号
S1022
激活
S1024
请求发送电池ID和公钥（证书）
S1030
使用签名私钥82对认证公钥74加密
S1134
向发行了签名验证公钥84的电子证书的认证机构请求电子签名的有效性的确认
S1132
发送电池ID、认证公钥74的电子证书（包含认证公钥74的明文和加密的认证公钥74）和签名验证公钥84的电子证书
S1040
使用签名验证公钥84，对利用签名私钥82加密的认证公钥74进行解密
S1042
比较明文的认证公钥74和解密的认证公钥74
S1044
在两者匹配的情况下，保存认证公钥74
结束
结束

图11

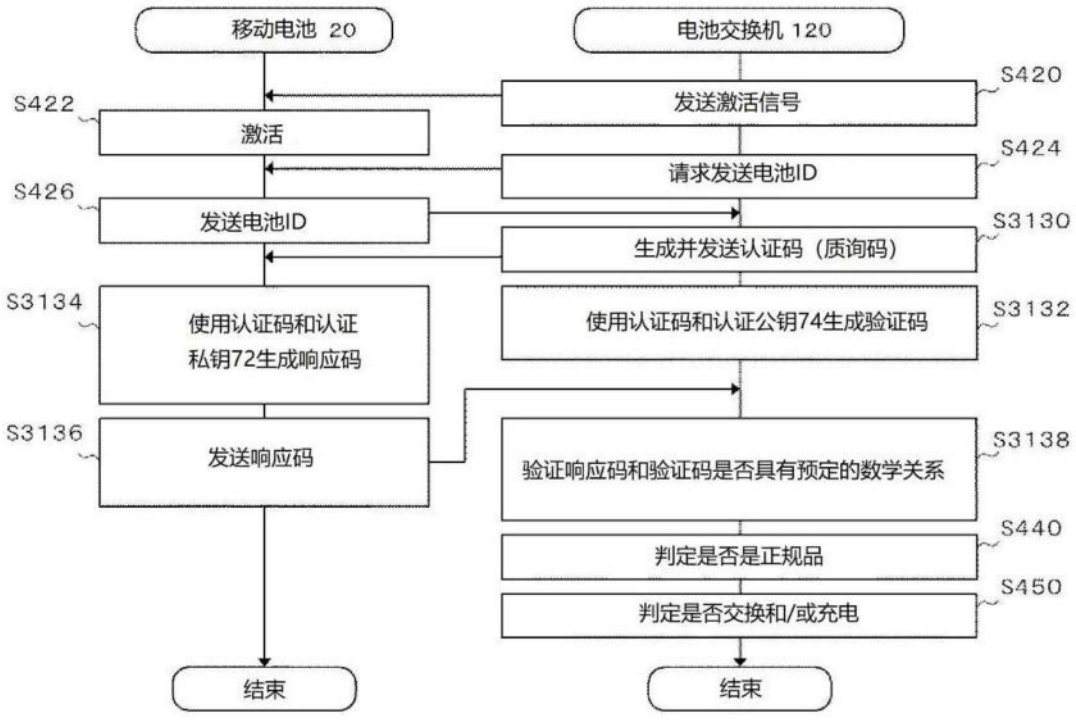

移动电池 20
电池交换机 120
S420
发送激活信号
S422
激活
S424
请求发送电池ID
S426
发送电池ID
S3130
生成并发送认证码（质询码）
S3134
使用认证码和认证私钥72生成响应码
S3132
使用认证码和认证公钥74生成验证码
S3136
发送响应码
S3138
验证响应码和验证码是否具有预定的数学关系
S440
判定是否是正规品
S450
判定是否交换和/或充电
结束
结束

图12

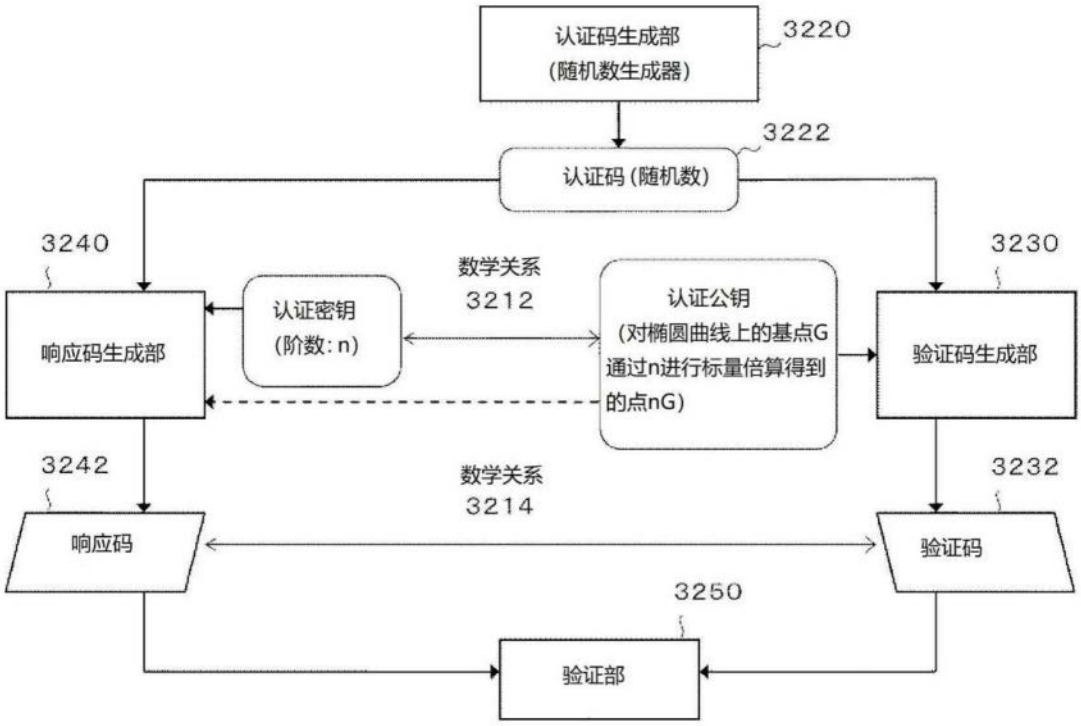

认证码生成部
(随机数生成器)
3220
3222
认证码(随机数)
3240
3230
数学关系
3212
响应码生成部
认证密钥
(阶数:n)
认证公钥
(对椭圆曲线上的基点G
通过n进行标量倍算得到
的点nG)
验证码生成部
3242
数学关系
3214
3232
响应码
验证码
3250
验证部

图13

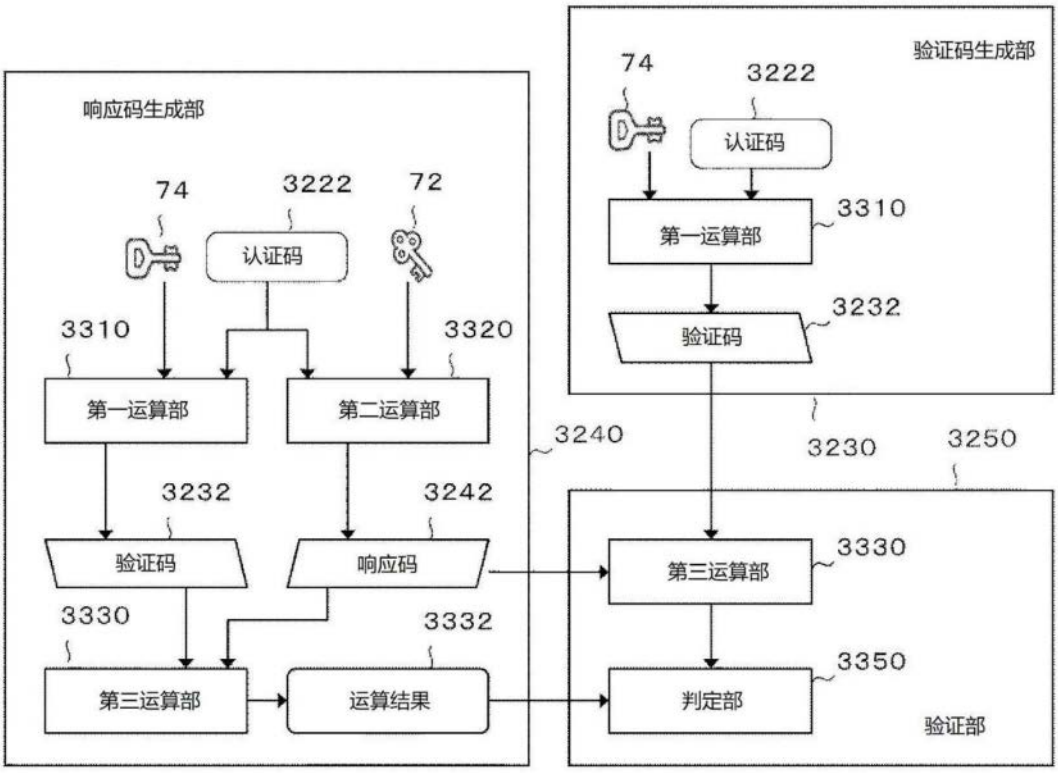

响应码生成部
74
3222
72
认证码
3310
3320
第一运算部
第二运算部
3232
3242
验证码
响应码
3330
3332
第三运算部
运算结果
验证码生成部
74
3222
认证码
第一运算部
3310
3232
验证码
3240
3230
3250
第三运算部
3330
判定部
3350
验证部

图14

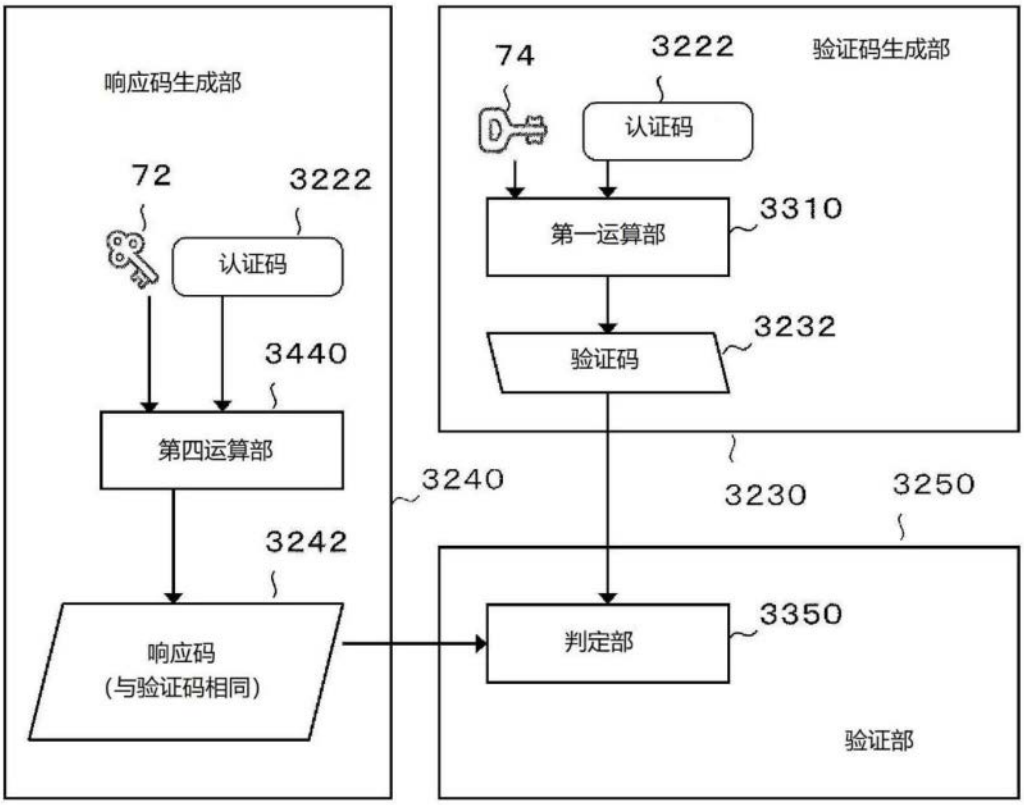

响应码生成部
72
3222
认证码
3440
第四运算部
3242
响应码
(与验证码相同)
3240
74
3222
验证码生成部
认证码
3310
第一运算部
3232
验证码
3230
3250
3350
判定部
验证部

图15

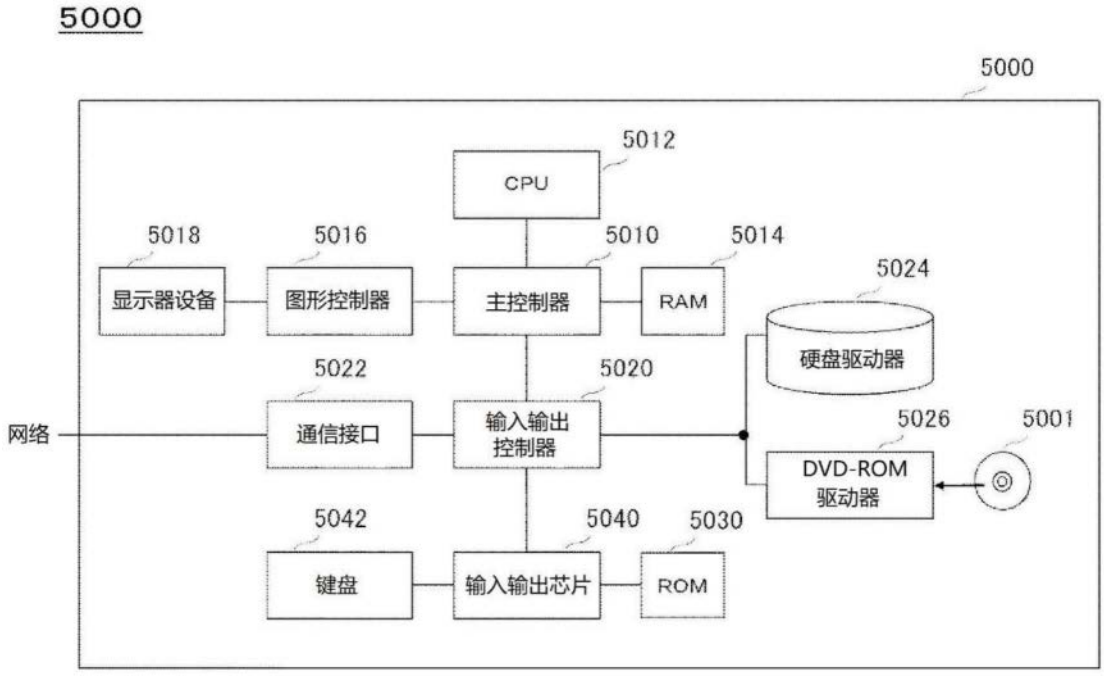

5000
5000
5012
CPU
5018
显示器设备
5016
图形控制器
5010
主控制器
5014
RAM
5024
硬盘驱动器
5022
通信接口
网络
5020
输入输出
控制器
5026
DVD-ROM
驱动器
5001
5042
键盘
5040
输入输出芯片
5030
ROM

图16