201716677

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201716677 A

(43)公開日： 中華民國 106 (2017) 年 05 月 16 日

(21)申請案號：105121472 (22)申請日： 中華民國 105 (2016) 年 07 月 06 日

(51)Int. Cl.： *E05B47/06 (2006.01)* *G07C9/00 (2006.01)*

(30)優先權：2015/07/06 美國 62/189,195

(71)申請人：艾克瑟斯智權控股公司 (黎巴嫩) ACSYS IP HOLDING INC. (LB)
黎巴嫩

(72)發明人：麥甘克 大衛 MEGANCK, DAVID (BE)；貝爾哈迪亞 卡利 BELHADIA, KARIM (FR)；莫拉狄恩 珍 MOURADIAN, JEAN (CA)；法里斯 阿麥德 FARES, AHMAD (LB)

(74)代理人：楊長峯；李國光；張仲謙

申請實體審查：無 申請專利範圍項數：20 項 圖式數：10 共 89 頁

(54)名稱

用於具有冗餘訪問控制的安全鎖系統之系統及方法

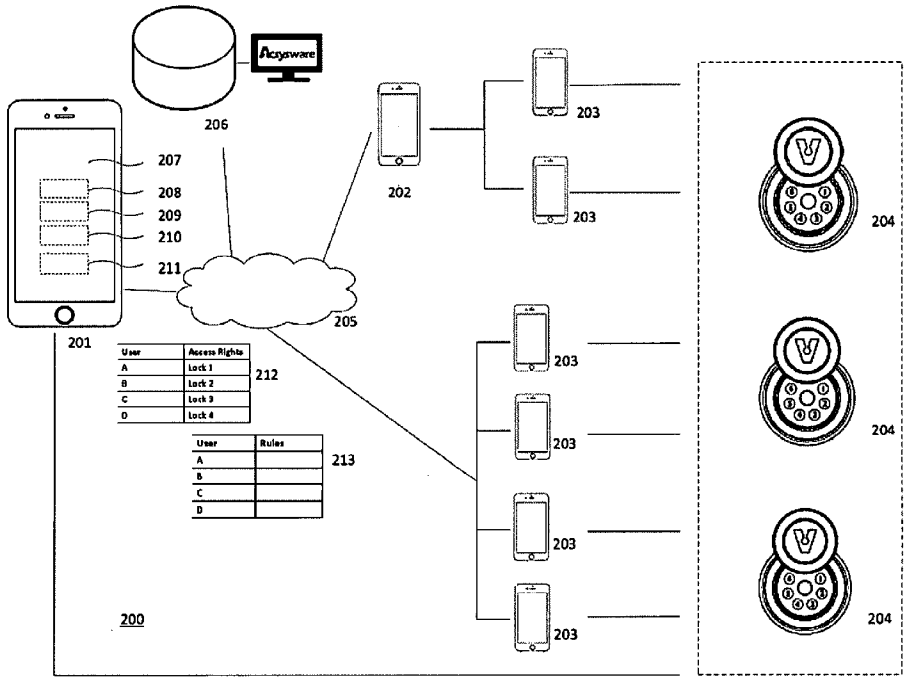
SYSTEMS AND METHODS FOR SECURE LOCK SYSTEMS WITH REDUNDANT ACCESS CONTROL

(57)摘要

揭露一種用於提供具有冗餘訪問通道的安全鎖具之系統及方法。在本發明的一些實施例中，智慧鎖具具有硬體處理器、電源、鎖芯、形成凸部旋鈕的鈕件及凸部保護件。凸部旋鈕與凸部保護件保護及隱藏硬體處理器、電源及鎖芯。凸部保護件形成與凸部旋鈕滑動地互鎖的環形槽。凸部旋鈕具有用於接受認證資訊之複數個冗餘訪問通道。冗餘訪問通道可包括接收生物辨識資訊的生物辨識掃描器、輸入許可證的通行碼按鍵區或接收來自行動裝置的許可證及傳輸回應給行動裝置的無線收發器。當使用者不能透過第一冗餘訪問通道打開鎖具時，智慧鎖具係配置成允許透過第二訪問通道進行訪問。

Systems and methods for providing secure locks having redundant access channels are disclosed. In some embodiments of the invention, the smart lock has a hardware processor, a power source, a cylinder, a button that forms a rose knob, and a rose protector. The rose knob and rose protector protect and conceal the hardware processor, the power source, and the cylinder. The rose protector forms an annular groove that slidably interlocks with the rose knob. The rose knob has a plurality of redundant access channels for receiving authentication information. The redundant access channels may include a biometric scanner for receiving biometric information, a passcode keypad for entering a token, or a wireless transceiver for receiving a token from a mobile device and transmitting a response to the mobile device. When the user cannot open the lock through the first redundant access channel, the smart lock is configured to allow access through a second access channel.

指定代表圖：



第 2A 圖

符號簡單說明：

200・・・訪問控制系統

201・・・主管者裝置

202・・・管理者裝置

203・・・使用者裝置

204・・・智慧鎖具

205・・・中心訪問伺服器

206・・・遠端伺服器

207・・・螢幕顯示器

208・・・儲存媒體

209・・・處理器

210・・・無線收發器

211・・・NFC 元件

212・・・規則

213・・・訪問權

201716677
專利案號：105121472

申請日：105.7.6
IPC分類：E05B 47/06 (2006.01)
G07C 9/00 (2006.01)

201716677

【發明摘要】

【中文發明名稱】用於具有冗餘訪問控制的安全鎖系統之系統及方法

【英文發明名稱】Systems And Methods For Secure Lock Systems With Redundant Access Control

【中文】

揭露一種用於提供具有冗餘訪問通道的安全鎖具之系統及方法。在本發明的一些實施例中，智慧鎖具具有硬體處理器、電源、鎖芯、形成凸部旋鈕的鈕件及凸部保護件。凸部旋鈕與凸部保護件保護及隱藏硬體處理器、電源及鎖芯。凸部保護件形成與凸部旋鈕滑動地互鎖的環形槽。凸部旋鈕具有用於接受認證資訊之複數個冗餘訪問通道。冗餘訪問通道可包括接收生物辨識資訊的生物辨識掃描器、輸入許可證的通行碼按鍵區或接收來自行動裝置的許可證及傳輸回應給行動裝置的無線收發器。當使用者不能透過第一冗餘訪問通道打開鎖具時，智慧鎖具係配置成允許透過第二訪問通道進行訪問。

【英文】

Systems and methods for providing secure locks having redundant access channels are disclosed. In some embodiments of the invention, the smart lock has a hardware processor, a power source, a cylinder, a button that forms a rose knob, and a rose protector. The rose knob and rose protector protect and conceal the hardware processor, the power source, and the cylinder. The rose protector forms an annular groove that slidably interlocks with the rose knob. The rose knob has a plurality of

redundant access channels for receiving authentication information. The redundant access channels may include a biometric scanner for receiving biometric information, a passcode keypad for entering a token, or a wireless transceiver for receiving a token from a mobile device and transmitting a response to the mobile device. When the user cannot open the lock through the first redundant access channel, the smart lock is configured to allow access through a second access channel.

【指定代表圖】　第2A圖

【代表圖之符號簡單說明】

200：訪問控制系統

201：主管者裝置

202：管理者裝置

203：使用者裝置

204：智慧鎖具

205：中心訪問伺服器

206：遠端伺服器

207：螢幕顯示器

208：儲存媒體

209：處理器

210：無線收發器

211：NFC 元件

212：規則

213：訪問權

【特徵化學式】

無

【發明說明書】

【中文發明名稱】用於具有冗餘訪問控制的安全鎖系統之系統及方法

【英文發明名稱】 Systems And Methods For Secure Lock Systems With Redundant Access Control

【技術領域】

【0001】 相關申請案的交互參照。

【0002】 本申請案主張於2015年7月6日向美國智慧財產局申請之美國臨時專利申請案第62/189,195號，其全部內容於此併入作為參考。本申請案關於於2016年3月3日向美國智慧財產局申請之美國專利申請案第15/060,237號及於2016年5月5日向美國智慧財產局申請之美國專利申請案第15/147,759號，其全部內容於此亦併入作為參考。

【0003】 本發明關於鎖具及行動裝置，而且更具體而言是關於用於具有冗餘通道的訪問之安全鎖及訪問控制系統之方法及系統。

【先前技術】

【0004】 訪問控制(access control)市場持續關注在將生物辨識(biometric)或無線通訊技術整合至鎖具系統的改善，以形成一般稱為機電鎖具或智慧鎖具。智慧鎖具一般可分為兩類：1)鎖芯類型(cylinder-based)智慧鎖具；2)表面安裝的智慧鎖具。

【0005】 鎖芯類型智慧鎖具通常提供有包括無線讀取機的可移除鈕。此無線鈕件讀取機係配置成接收及處理自使用者裝置，例如，無線射頻辨識(RFID)

允許智慧卡或RFID允許智慧手機等傳送的無線訊號。此種卡類型或手機類型的無線裝置當可使用作為鑰匙，以獲得對一或多個鎖具的訪問。在處理自使用者裝置接收的無線訊號之後，無線鈕件讀取機通常傳送指示及資訊至電子設備的鈕件或機電鎖具的鎖芯(cylinder)。當使用者具有足夠的憑證時，鈕件或鎖芯將接著啟動鈕件或鎖芯中的另一裝置，以允許使用者藉由往順時針方向或逆時針方向轉開鈕件以打開機電鎖具。轉動鈕件因而允許使用者接合或脫離機電鎖具的門栓(deadbolt)。鎖芯類型的RFID鎖的的優點之一係為容易安裝，並且在多數情況不需佈線及由電池操作，使其可在一段期間自主運作。

【0006】現今可用的另一類鎖具包括由RFID讀取機、生物辨識讀取機、密碼類型讀取機或其組合所控制的表面安裝智慧鎖具。部分的該鎖具進一步包括可以可與鎖具擁有者無線通訊的嵌入式無線通訊接收器。然而，這些鎖具通常需要複雜且侵入式的安裝過程，如鑽孔或切入門框等。因此，此表面安裝智慧鎖具可能如同其安裝一樣難以被移除。再者，表面安裝鎖具通常依靠電池作為電源。然而，鎖具對電池的依賴性而使其容易受電池耗盡或故障的影響。雖然許多表面安裝智慧鎖具具有在電池故障狀況時的隱藏機械鑰匙補償，但由於這些補償可能因簡單的撞擊、剔除或鑽孔而為不安全的。一但被撞擊、剔除或穿孔，意圖增強鎖具的安全性之其他冗餘安全特徵，例如生物辨識掃描器將變得無效。

【0007】具有RFID鈕件鎖的鎖芯類型智慧鎖部分地因其安裝方式而同樣易受破壞。實際上，如第1A圖繪示，在現今可得的部分產品上的無線讀取機鈕件108通常藉由樞軸或金屬棒102接附於機電型鎖芯101。當未使用時，此樞軸或金屬棒102通常為自由地旋轉，其避免惡意使用者損毀或破壞鎖具100。特別是，

當有害的入侵者對鈕件簡單地施加大力的旋轉力時，部分機電鎖芯可能變得失效，而使有害的入侵者進出使用者的家。由於自由旋轉樞軸，機電鎖芯通常將不會因蠻力旋轉力而變得失效。如第1A圖繪示，樞軸102通常為將鈕件上的電子裝置103至105耦接到機電鎖芯106內的電子裝置之窄導電管。指令傳送至接合或脫離鈕件的機電鎖芯101，接著將鎖芯門栓進行接合或脫離，因而對使用者提供進出。

【0008】 此外，整合無線通訊能力通常需要對鎖具附加持續且可靠的電源。舉例來說，如第1A圖所示的無線鈕件一般具有單一電源105。為了避免破壞，單一電源105通常配置在設置於門的內側表面之上的鈕件108的內側。然而，這些電源105可能失去電力或遭受其他無預期的故障。當電源105耗盡或故障時，使用者通常需要去呼叫專業鎖匠以更換電源或切開、鑽孔及破壞門框109整體。雖然部分鎖具已經附加替換供應電源，以從門的外側表面向內側鈕件108供電，該裝置通常位於由鎖固定或不容易獲得的空間中。

【0009】 使用無線射頻辨識(RFID)的鎖芯類型智慧鎖具存在其他缺點。一般來說，無線射頻辨識(RFID)鎖芯類型智慧鎖具使用已知易受駭侵(hacking)或逆向工程的被動無線射頻辨識(RFID)技術。再者，被動無線射頻辨識技術在使用者裝置110(如，RFID允許卡片或RFID允許智慧手機)遺失或被偷竊的狀況中缺乏彈性。在這些狀況中，關於使用者的RFID允許卡片或具有RFID允許智慧手機的資訊將需要從鎖具的記憶體中物理性刪除。這通常需要系統管理者或鎖匠移動至鎖具的所在位置並物理性更新鎖具中的記憶體及任何相關的電子裝置。因為系統管理者或鎖匠將需要對各鎖具重複此處理，若遺失或遭偷竊的RFID允許卡片配置成訪問大量的鎖具時，可能顯著地增加更新此系統的費用。

【0010】再者，因為這些鎖具通常不提供針對開鎖的替代冗餘訪問(redundant access)通道，而可能阻止使用者訪問位置並被鎖在門外，直到提供替代的RFID允許卡片、更新RFID允許鎖具或找到具有鎖具憑證的其他人。同樣地，若使用者的手機電池耗盡或手機關機時，由於RFID特徵可能無法運作，而使依賴RFID允許智慧手機的使用者可能被鎖在門外。

【0011】在各國家及人口區的大量使用者至今仍未擁有或具有對手機的訪問。因此，只依賴RFID允許智慧手機之許多解決方法係為不可行的。部分製造商已將生物辨識讀取機或進入訪問密碼的按鍵區併入至訪問控制系統，以試圖對沒有智慧手機的訪問之使用者提供解決方法。然而，由於使用在生物辨識讀取機或密碼類的解決方法之元件的尺寸、價格及電力限制，而可能限制由這些替代訪問通道所提供的安全之品質及程度。

【0012】使用在連接這些替代訪問通道的憑證(例如，指紋或固定數字通行碼)可儲存在嵌入於鎖具的局部記憶體。因此，新使用者的登錄通常需要使用者實際地出現在鎖具的地點，以輸入他或她的憑證(例如，指紋或固定數字通行碼)，或經由可攜式記憶裝置傳輸(例如，USB快閃裝置)而具有他或她的憑證。在任一情況下，系統管理者可能需要實際出現在鎖具，以在鎖具上手動傳輸使用的憑證。在使用者不再需要對任何鎖具訪問的情況下，可需要另外實地訪問以更新鎖具而從鎖具移除使用者的憑證及訪問資訊。

【0013】這些系統的另一個缺點係缺乏對於暫時限制訪問鎖具的控制。亦即，一旦對鎖具的訪問賦予使用者(例如，藉由於鎖具上輸入他或她的通行碼或指紋)時，則難以控制使用者何時可訪問鎖具。一般來說，這些系統的使用者可無時無刻地對鎖具進行訪問。於是，大多數這些裝置也未保存提供鎖具使用的

資訊的各種事件或活動的使用日誌。因此，鎖具擁有者或系統管理者通常無法分析關於何時使用特定鎖具及何者試圖使用鎖具的資訊。

【0014】雖然一些鎖具儲存包含使用資訊的日誌，其通常儲存位在鎖具的記憶體系統，而因此可能需要管理者實地訪問鎖具以電性傳輸日誌。一些製造商以允許鎖具將資訊無線通訊到裝置，如使用者的智慧手機。然而，這些鎖具受到如上所述的類似能量限制。特別是，鎖具中的無線通訊裝置在傳送及接收數據時消耗大量的能量。因此，由電池供電的無線通訊裝置僅可在耗盡及用盡之前的有限時間下進行操作。

【0015】與鎖芯類型的RFID鈕件鎖具相比，機械鎖具通常不具有凸出鈕件且因此不易有相同程度的破壞。再者，其不受電源供應故障的影響。然而，機械鎖具因其設計而易受其他工具攻擊，可能使具有惡意的人藉由自該行業可得到的各種道具破壞、拔取、鑽孔或切割鎖芯而進出屋內。

【0016】為了保護鎖具免於此破壞，一些機械鎖具製造商提供對抗此破壞的保護裝置，稱為防鑽孔凸部(anti-drilling rose)111。防鑽孔凸部通常附加在門的外面側上的鎖芯面。如第1A圖繪示，防鑽孔凸部通常係由耐久材料所製造之堅固外殼，其覆蓋鎖芯的暴露部分。防鑽孔凸部通常從門的內側向外旋入112到位，其避免從門的外部任意拆卸系統，但允許從門的內側拆拆卸。防鑽孔凸部111通常為耐久的而足以抵擋可能破壞機械鎖的以鐵鎚的鈍擊、用特殊鉗子拔取以及鑽孔。然而，由於其通常具有自由旋轉的防鑽孔保護盤，而阻止鎖具及鑰匙的正常使用，因而防鑽孔凸部通常無法附加至機械鎖芯。再者，儘管防鑽孔凸部提供安全性保護的加強，然而其被認為在外觀上不佳，而因此不常使用。

【0017】 RFID鈕件鎖具通常不具有防鑽孔凸部。因此，其無法對抗側向推力，如鐵鎚的大的側向推力，其可能使鈕件從鎖芯主體位移。當鈕件從鎖芯主體位移時，鎖具可遭到破壞或不可操作，或鎖具可遭到破壞且惡意使用者可進出屋內。

【0018】 現今在市場上具有使用藍牙技術以在鎖具和智慧型手機之間進行通訊之多種裝置。然而，因為惡意者可截取及解碼在手機和鎖具之間通訊的藍牙訊號，因而藍牙通訊也可能容易受到駭侵攻擊。

【0019】 因此，需要一種更安全的無線鎖芯類型智慧鎖具的解決方案，其可藉由卡片、智慧手機或藉由其他冗餘手段，如生物辨識讀取機或訪問密碼進行打開或操作。解決方案亦應藉由智慧手機應用程式、行動裝置或電腦進行管理，其使鎖具擁有者無線且即時地對鎖具及使用者控制訪問權(access rights)。對訪問權的控制應允許系統擁有者給予使用者選擇性許可，例如藉由提供部分使用者具有無限制的訪問鎖具權及其他使用者具有時間限制或單一使用的訪問權。解決方案亦應可抵擋各種形式的物理性破壞及損害，而提供高度安全性。解決方案也應併入冗餘電源，以預防電源故障且在電源故障時不包括機械補償(mechanical override)。

【發明內容】

【0020】 在各種實施例中，本發明提供用於控制及監視訪問控制系統的系統、方法及設備。根據本發明的一些實施例，訪問控制系統包括提供冗餘訪問控制的智慧鎖具。智慧鎖具包括儲存媒體、電源、硬體處理器、具有接合門栓的凸輪部(cam)之鎖芯、及接合凸輪部以解鎖門栓的鈕件。

【0021】鈕件包括接收認證資訊的複數個冗餘訪問通道。冗餘訪問通道包括接收生物辨識資訊的生物辨識掃描器、通行碼按鍵區及/或接收從行動裝置的許可證(token)及傳輸回應給行動裝置的無線收發器。

【0022】智慧鎖具配置成基於管理者決定的一組規則驗證從通行碼按鍵區、生物辨識掃描器及/或行動裝置接收的認證資訊，且當使用者透過複數個冗餘訪問通道的第一通道來認證時，則解鎖門栓。當使用者無法通過第一通道打開智慧鎖具時，智慧鎖具可允許透過複數個冗餘訪問通道的第二通道進行訪問。以此方式，當使用者不再使用第一通道訪問智慧鎖具時，使用者可使用第二通道打開鎖具。

【0023】訪問控制系統可包括一個或多個智慧鎖具。系統可藉由使用者對智慧鎖具請求訪問而進行訪問及藉由主管者(masters)或管理者(administrators)對智慧鎖具限制訪問而控制。在一些實施例中，使用者可訪問，及主管者或管理者可接近即時地從其各自的行動裝置控制對智慧鎖具的訪問。主管者或管理者可使用行動裝置以配置規則及訪問權，以控制如何及何時使用者可打開智慧鎖具。以此方式，訪問控制系統可提供以允許主管者或管理者不需於門或鎖具上安裝有線網路(hard-wired internet)或數據連接而接近即時控制及監視使用者。因為鎖芯適用於配合標準插槽，而不需修改或再加工門框或鎖具系統

【0024】在本發明的部分態樣，主管者或管理者可配置規則及訪問權，以限制使用者如何訪問智慧鎖具。訪問權指定使用者可訪問的鎖具，及配置規則指定在打開智慧鎖具前必須滿足的條件。規則因此允許主管者或管理者基於地點及時間限制使用者的訪問。以此方式，主管者或管理者可精確控制使用者可如何打開智慧鎖具。

【0025】主管者或管理者可要求使用者在每次意圖打開智慧鎖具時請求通行碼或許可證。當使用者提出請求時，主管者或管理者可接近即時接收請求及決定是否允許使用者的訪問。主管者或管理者可要求使用者提供額外的認證資訊，如密碼以確認使用者的身分。若主管者或管理者決定允許使用者的訪問，則接近即時傳輸通行碼或許可證給使用者。在一些實施例中，請求可根據觸發事件而被傳送。因此，主管者或管理者可根據個例控制使用者的訪問。

【0026】通行碼可為固定的或動態的。動態的通行碼可使主管者或管理者允許使用者單一使用或限制時間訪問鎖具。通行碼可從行動裝置無線地提供給鎖具或手動輸入到按鍵區。因此，即使無法使用使用者的行動裝置，使用者可以通行碼訪問鎖具。

【0027】在本發明的一些實施例中，智慧鎖具的無線收發器配置成直接且接近即時地與行動裝置、以及網路裝置、控制訪問伺服器或管理者裝置通訊。接著，鎖具可從網路裝置、控制訪問伺服器或管理者裝置接收通訊，以指示鎖具允許或拒絕使用者訪問。

【0028】根據本發明的一些實施例，智慧鎖具包含配置成創造行動寬頻連接(cellular broadband connection)及接近即時與管理者裝置或中心訪問伺服器通訊的無線數據機。當鎖具接收許可證、生物辨識掃描或通行碼時，其可基於一組配置規則傳輸用於訪問鎖具的需求。接著，鎖具可接近即時接收自管理者裝置或中心訪問伺服器的指示以允許或拒絕訪問的請求。以此方式，當使用者的行動裝置無法與管理者裝置或中心訪問伺服器通訊時，鎖具可藉由其本身建立與管理者裝置或中心訪問伺服器的連結。因此，鎖具可不依靠使用者的行動裝置中繼(relay)通訊而與管理者裝置或中心伺服器通訊。

【0029】 在本發明的其他實施例，智慧鎖具亦可配置成與網路裝置通訊，其向管理者裝置或中心訪問伺服器中繼通訊。網路裝置可為無線接收器、路由器、中繼器或使用相似領域的無線傳輸器或用於建立短程無線連接的無線區域網路(LAN)等的類似裝置。因此，智慧鎖具可相似地創造不依靠使用者的行動裝置中繼通訊而與管理者裝置或中心訪問伺服器通訊之連結。

【0030】 智慧鎖具可包括慣性模組。慣性模組配置以決定門的狀態，其表示門是否打開或關閉。鎖具可相似地配置以決定門栓的狀態，其表示門栓的鎖住或解鎖位置。鎖具可接近即時通訊門的狀態及門栓的狀態至管理者裝置或中心訪問伺服器。因此，管理者裝置或中心訪問伺服器可決定門是否已經維持打開、關上、鎖住或解鎖。

【0031】 根據本發明的一些實施例，智慧鎖具的鈕件為可移除的或可充電的。鈕件可包括匹配充電站的充電介面之充電介面。當鈕件的電量低下時，使用者可移除鈕件並藉由充電站充電鈕件。在本發明的更進一步的實施例中，鈕件可包括允許使用者從例如外部裝置或充電站供電給鈕件的輸入/輸出(I/O)埠。輸入/輸出埠進一步允許使用者提取(retrieve)儲存在鈕件的訪問資訊。因此，當鈕件在充電站充電時，充電的鈕件可透過輸入/輸出埠提取儲存在鈕件的訪問資訊。在一些實施例中，充電站耦接到網路連接，而將訪問資訊通訊至管理者裝置或中心訪問伺服器。

【0032】 根據本發明的一些實施例，鎖具進一步包括凸部(rose)保護件及鈕件形成凸部旋鈕(rose knob)。凸部保護件(rose protector)及凸部旋鈕保護及隱藏硬體處理器、電源及鎖芯。凸部保護件具有形成用於與凸部旋鈕互鎖的環狀槽之外壁及內壁。內壁實質上相對於門垂直地形成，而外壁形相對於門形成錐形。

由於外壁的錐形形狀，環狀槽具有沿著垂直於(normal to)門的平面而漸少的漸變厚度。以此方式，錐形外壁的形狀偏轉蠻力(brute force)的撞擊。

【0033】該凸部旋鈕具有外表面及內表面。外表面及內表面形成用來與凸部保護件的環狀槽互鎖的環狀邊緣、及包括電源、硬體處理器及用於接收認證資訊之冗餘訪問通道的開口。環狀邊緣具有與環狀槽的漸變厚度匹配的厚度。

【0034】凸部保護件具有用於一個或多個固定桿及一個或多個緊固件的一組通孔，以將凸部保護件固定於門。因此，當凸部旋鈕的邊緣與凸部保護件的環狀槽滑動地互鎖時，凸部旋鈕為不可移動地固定於凸部保護件。凸部旋鈕為可自由地旋轉直到驗證自通行碼按鍵區、生物辨識掃描器或行動裝置接收認證資訊，此時凸部旋鈕配置成啟動凸輪部以解鎖門栓。凸部旋鈕及凸部保護件由堅固材料，如不鏽鋼構成，及可具有減少表面的摩擦係數之平滑表面(finished surface)。以此方式，凸部旋鈕或凸部保護件避免破壞及損害。

【圖式簡單說明】

【0035】本發明的目的及特徵可藉由參考下列詳細敘述及附圖而更進一步理解。

【0036】第1A圖及第1B圖繪示例示性無線讀取鈕件及反鑽孔凸部的配置。

【0037】第2A圖、第2B圖、第2C圖及第2D圖係根據本發明的實施例繪示訪問控制系統。

【0038】第3A圖、第3B圖、第3C圖、第3D圖、第3E圖、第3F圖、第3G圖及第3H圖係根據本發明的實施例繪示使用在訪問控制系統的智慧鎖具。

【0039】第4圖係根據本發明的實施例繪示具有可充電電源的智慧鎖具。

【0040】第5圖係根據本發明的實施例繪示打開智慧鎖具的過程。

【0041】 第6圖係根據本發明的實施例繪示在訪問控制系統登錄觸發事件的過程。

【0042】 第7圖係根據本發明的實施例繪示在訪問控制系統中控制智慧鎖具的訪問之過程。

【0043】 第8A圖、第8B圖、第8C圖、第8D圖及第8E圖係根據本發明的實施例繪示用於在訪問控制系統中控制智慧鎖具的訪問的介面。

【0044】 第9A圖、第9B圖、第9C圖、第9D圖、第9E圖及第9F圖係根據本發明的實施例繪示用於在訪問控制系統中控制智慧鎖具的介面。

【0045】 第10圖的10A、10B、10C部分係根據本發明的實施例繪示用於在訪問控制系統中訪問智慧鎖具的使用者介面。

【實施方式】

【0046】 本發明的實施例包括可使使用者使用冗餘訪問通道打開鎖具、及允許主管者或管理者接近即時控制使用者訪問之系統、方法及設備。

【0047】 第2A圖及第2B圖繪示例示性訪問控制系統接近即時通訊使用資訊，同時提供訪問的冗餘通道給使用者。該系統包括一個或多個智慧鎖具204、中心訪問伺服器205及用於訪問及控制智慧鎖具的裝置201、202及203。使用者透過如下更詳細描述的一個或多個冗餘通道打開智慧鎖具204。主管者與管理者自主管者裝置201或管理者裝置202控制使用者如何訪問智慧鎖具204。使用者可與主管者、管理者通訊，並且從使用者裝置203打開智慧鎖具。使用者也可不需任何使用者裝置203而手動打開智慧鎖具。中心訪問伺服器205中繼及儲存在使用者和主管者或管理者接近即時交換的資訊。將注意的是，「接近即時(near

real-time)」通訊可表示即時或實質上即時發生的通訊，但由於網路基礎建設而經歷輕微、不明顯或不顯著的延遲。當使用者可能因例如，訪問通道無效或變得無法操作而不再透過訪問通道之其一打開智慧鎖具時，使用者可經由其他可用的訪問通道打開智慧鎖具。因此，訪問控制系統200可讓使用者使用冗餘訪問通道打開智慧鎖具，並且允許主管者或管理者接近即時控制使用者訪問。

【0048】 主管者裝置201及管理者裝置202建立及指定規則和訪問權給意圖獲得一個或多個智慧鎖具204的訪問之使用者。訪問權辨識各使用者被授權以打開的智慧鎖具204。在允許使用者打開智慧鎖具204之前，必須滿足的規則及條件。舉例來說，訪問權可藉由主管者裝置201或管理者裝置202配置，以指定使用者可打開的智慧鎖具204群，並且規則指定允許使用者打開特定智慧鎖具的日期及時間。

【0049】 如第2B圖繪示，主管者裝置201及管理者裝置202也配置成指定使用者可使用於提供認證資訊的訪問通道，以打開智慧鎖具204。如下更詳細地說明，訪問通道可例如為掃描生物辨識資訊到生物辨識掃描器214、輸入通行碼在按鍵區215或從行動裝置216無線傳輸許可證。智慧鎖具可提供任意或所有訪問通道的結合給使用者。舉例來說，通常或預設使用的第一訪問通道可從使用者的行動裝置216無線傳輸的許可證，及第二訪問通道和第三訪問通道可分別為生物辨識掃描器214和通行碼按鍵區215，以在第一訪問通道對使用者無效的情況下使用。

【0050】 主管者裝置201、管理者裝置202或使用者裝置203可為行動裝置、軟體服務或軟體應用程式。行動裝置可例如為智慧手機、平板電腦或手持裝置。行動裝置包括觸控式螢幕顯示器207、儲存媒體208及處理器209。在一些

實施例中，行動裝置包括用於傳輸及接收無線射頻辨識(RFID)、雜訊回授編碼(NFC)或藍芽訊號的無線收發器210、或透過行動裝置的行動連接或網路連接。

【0051】 中心訪問伺服器205可為雲端類型伺服器及可連接至遠端伺服器206。遠端伺服器206可包括具有客服人員的客服中心，以接收使用者的電話及訪問請求。

【0052】 在本發明的一些實施例中，行動裝置包括NFC元件211，其可為配備有NFC發射器的SIM卡或SD卡。NFC允許的SD卡可置入的行動裝置的SD卡槽，以提供具有NFC通訊功能的智慧型手機。相似地，NFC允許的SIM卡可置入的行動裝置的SIM卡槽，以提供具有NFC通訊功能的智慧型手機。

【0053】 如第2A圖繪示，訪問控制系統中的個體可具有不同角色。舉例來說，個體可為主管者、管理者或使用者。主管者可增加、移除及配置管理者或使用者的訪問權。管理者同樣可增加、移除及配置使用者的訪問權。使用者係為意圖訪問由智慧鎖具保全的地點的個體。個體的訪問權可配置給各使用者或管理者，或更一般水平配置給使用者群或管理者群。同樣地，可給予使用者或管理者特定智慧鎖具或智慧鎖具群的訪問。

【0054】 舉例來說，在訪問控制系統的商業設定，主管者裝置201或管理者裝置202可由期望控制他們的員工如何及何時訪問企業區域的監督者或經理操作。商業經理可指定監督者作為管理者，其可進一步指定一組員工為訪問特定智慧鎖具群的使用者。另一個例子，在住家設定中，主管者裝置201或管理者裝置202可由父母操作，以控制住家不同區域的進入者的訪問以及監視其訪問資訊。指定自己為主管者的父母可指定他們的保姆作為管理者以及他們的孩子作為使用者，以及指定保姆及孩子可訪問的住家區域及其如何或何時可進出該區

域。如下更詳細地描述，監督者或父母可接收員工、保姆或孩子意圖訪問由智慧鎖具204控制的地點之警報或報告。

【0055】訪問控制系統的主管者或管理者配置使用者如何用一組規則212及訪問權213打開智慧鎖具。訪問權213在訪問控制系統中辨識各個體或個體群，以及在訪問控制系統中的各智慧鎖具或智慧鎖具群。訪問權213亦將各個體與智慧鎖具相聯繫。一組規則212指定可用於打開智慧鎖具的訪問通道，及(若需要時)要求以允許個體打開智慧鎖具的條件。舉例來說，指定自己作為主管者的父母可配置針對保姆的訪問權及規則，而使保姆可使用通行碼或生物辨識掃描打開智慧鎖具。該規則可進一步配置條件，而使保姆只可在一週的某些天打開智慧鎖具、或父母核准各請求訪問之後，才可打開智慧鎖具。

【0056】訪問權及規則可儲存在主管者、管理者、使用者、智慧鎖具或中心訪問伺服器的行動裝置。如下更詳細地描述，主管者或管理者可從主管者裝置201、管理者裝置202或中心訪問伺服器205中建立、修改或刪除訪問權及規則。當主管者或管理者建立、修改或刪除訪問權及規則時，訪問權或規則可通訊給中心訪問伺服器或使用者的行動裝置。使用者的行動裝置即可傳輸訪問權或規則給智慧鎖具做為部分的許可證。當使用者企圖打開智慧鎖具時，訪問權及規則可從行動裝置或智慧鎖具進行確認。舉例來說，當使用者提供通行碼或生物辨識掃描時，智慧鎖具可確認訪問權及規則以確定使用者是否在特定天或時間被授權打開智慧鎖具。另一個例子，傳輸許可證給智慧鎖具之前，使用者的行動裝置可確認訪問權及規則，以確定使用者是否被授權打開特定的智慧鎖具。當使用者未具有授權時，行動裝置將不傳輸許可證給智慧鎖具。在本發明

的一些實施例中，訪問權及規則可從主管者裝置201、管理者裝置202或中心訪問伺服器205確認。

【0057】智慧鎖具可安裝以保全地點之特定區域或房間，讓主管者或管理者精準控制個體可進行訪問的地點。舉例來說，在基地台中，智慧鎖具可安裝在設施的前門、儲存室的門及機櫃的門，其確保通常成為偷竊目標之電池、銅纜線、電子裝置及其他資產。商業經理(如，主管者)則可允許特定員工(如，使用者)進出設施，並且限制選定的少數員工進出儲存室及機櫃的門。如上所述，商業經理可進一步配置規則以指定員工如何訪問智慧鎖具及(若需要時)允許員工獲得訪問的條件。

【0058】另一個例子，地點的區域可例如為地下室、後院、浴室、前門、健身中心或車庫。因此，在住家設定中，父母可允許保姆訪問地下室、後院或父母的臥房，但只在保姆照顧小孩的特定時間間隔。如下所述，父母可進一步配置規則以允許保姆條件式訪問權，其要求保姆在每次意圖訪問智慧鎖具時請求許可。父母可進一步配置訪問權及規則，以允許孩子進出家裡的不同區域或房間，並且在提高的限制下。舉例來說，父母可配置訪問權及規則以拒絕孩子進出家裡的房間，如地下室、或如在一天的特定時間限制訪問區域，如健身中心。父母可進一步配置規則以規定孩子可使用於訪問區域的訪問通道，例如，使用兒童指紋以進出後院等。

【0059】根據本發明的一些實施例，使用者藉由從使用者的行動裝置的無線通訊216給智慧鎖具而打開一個或多個智慧鎖具204。藉由使用使用者的行動裝置之無線功能，智慧鎖具204可連接到中心訪問伺服器205而不需直接連結其

兩者之間。以此方式，可遠端控制智慧鎖具204的訪問而不需要在門框或鎖具上執行硬體有線系統。

【0060】 如上所述，智慧鎖具204可藉由從使用者的行動裝置無線傳輸許可證給智慧鎖具204而打開。許可證包含通行碼，其包括文字、數字、符號或其任意組合。通行碼可為動態或固定，如下更詳細地討論。智慧鎖具204根據由主管者或管理者決定的訪問權及規則並藉由比較接收的通行碼與儲存在智慧鎖具204的程序產生的通行碼來驗證許可證。若接收的通行碼由匹配程序產生的通行碼，則智慧鎖具204將接受許可證。智慧鎖具204將根據訪問權及規則以及許可證是否與藉由儲存程序產生的許可證匹配而向使用者行動裝置203通訊許可證是否已被驗證。此資訊可接著從使用者行動裝置203傳送到中心訪問伺服器205，其可作為通知或警報而中繼至主管者裝置201或管理者裝置202。

【0061】 主管者裝置201及管理者裝置202配置以指定使用者是否可使用者行動裝置的無線功能訪問智慧鎖具204及使用者具有何種訪問權。舉例來說，主管者裝置201及管理者裝置202可指定特定智慧鎖具204或一組智慧鎖具204的使用者訪問權為固定式或條件式。

【0062】 條件式訪問權允許主管者或管理者核准使用者打開智慧鎖具204的每次嘗試。舉例來說，當具有條件式訪問權的使用者嘗試訪問智慧鎖具204或一組智慧鎖具204時，系統將向主管者裝置201或管理者裝置202警告使用者203企圖訪問智慧鎖具204，並且接近即時請求主管者裝置201或管理者裝置202允許使用者訪問智慧鎖具204。接著，使用者可確定是否允許或拒絕使用者訪問。該確定可根據附加條件或驗證步驟。舉例來說，主管者或管理者可請求使用者提供證明使用者的身分或真偽，例如附加密碼的驗證資訊。另一個例子，因為使

用者未意圖訪問特定智慧鎖具204或未意圖在特定日期或時間訪問，管理者的主管者可拒絕使用者的訪問。若主管者或管理者決定應同意使用者訪問智慧鎖具204時，如下文詳細地描述，主管者裝置201或管理者裝置202則可提供使用者許可證。若主管者或管理者決定應拒絕使用者訪問智慧鎖具204時，主管者裝置201或管理者裝置202則不提供使用者許可證，且使用者將無法打開智慧鎖具204。以此方式，主管者裝置201或管理者裝置202可接近即時允許或拒絕智慧鎖具204的訪問。在一些實施例中，當主管者或管理者決定是否同意或拒絕使用者的訪問時，主管者裝置201或管理者裝置202將寄出警告給使用者，以通知使用者其訪問的請求已經同意或拒絕。

【0063】 固定訪問權允許使用者在沒有首先從主管者裝置201或管理者裝置202接收核准的情況下獲得對智慧鎖具204的訪問。舉例來說，使用者被授權固定訪問權而沒有限制地打開特定智慧鎖具204。此固定訪問可以固定通行碼提供，舉例來說，使用者可輸入在智慧鎖具204的按鍵區。接著使用者可以固定通行碼而在沒有首先從主管者裝置201或管理者裝置202接收接收核准的情況下打開智慧鎖具204。在一些實施例中，當具有固定訪問權的使用者已訪問或企圖訪問智慧鎖具204時，使用者的行動裝置203仍可通知主管者裝置201或管理者裝置202。舉例來說，在使用者輸入固定通行碼到智慧鎖具的按鍵區上之後，智慧鎖具可通訊給使用者的行動裝置智慧鎖，其已接收有效的固定通行碼並且解鎖智慧鎖具。接著，使用者的行動裝置可在使用者訪問及解鎖智慧鎖具204而接近即時地通知主管者裝置201、管理者裝置202或中心訪問伺服器205。

【0064】 主管者裝置201及管理者裝置202也可使用允許使用者以輸入在按鍵區215的通行碼或生物辨識掃描214打開一個或多個智慧鎖具204。這些訪問

通道可使使用者不使用行動裝置而獲得對智慧鎖具204的訪問，如下更詳細地描述，使用者可手動輸入通行碼或生物辨識掃描。以此方式，使用者可在沒有行動裝置、或行動裝置遺失、故障或其他無法無線傳輸許可證給智慧鎖具204的狀況下獲得對智慧鎖具204的訪問。因此，根據本發明的一些實施例，輸入通行碼或生物辨識掃描的按鍵區作為冗餘訪問通道，以提供使用者訪問智慧鎖具。在本發明的其他實施例中，輸入通行碼或生物辨識掃描的按鍵區可作為主要的或預設的訪問通道，並且從使用者行動裝置無線傳輸給智慧鎖具204可作為冗餘訪問通道。在進一步本發明的實施例中，使用者可能需要使用替代訪問通道的結合認證自己。舉例來說，在授權訪問鎖具之前，使用者可需要提供動態通行碼及指紋的結合。

【0065】 如上所述，許可證可包括可從使用者行動裝置203無線傳輸到智慧鎖具204的通行碼。如下更詳細地描述，通行碼亦可顯示在使用者裝置，以使用者可手動輸入通行碼在智慧鎖具204的按鍵區。智慧鎖具204藉由比較輸入的通行碼與藉由儲存在智慧鎖具204的程序產生的通行碼來認證固定通行碼。若程序產生匹配的通行碼，智慧鎖具204將授權使用者的訪問。

【0066】 在本發明的一些實施例中，通行碼可為密碼產生系統(CGS)產生的動態通行碼。動態通行碼係唯一的、單次使用、限制時間或一次性通行碼，其由中心訪問伺服器在請求時產生。通行碼部分根據請求通行碼的時間。

【0067】 根據本發明的一些實施例，提供使用者的通行碼的產生是根據關於使用者行動裝置之唯一資訊及請求或產生通行碼時間。對於行動裝置而言，通行碼可根據例如國際移動設備識別 (IMEI)、行動裝置的網路ID或兩個ID的結合及從行動裝置傳送請求的時間。

【0068】 或者，通行碼可為固定。未改變或未過期的固定通行碼可使用一次以上，及可在不需主管者或管理者的請求而獲得固定通行碼。期望避免固定通行碼被破解的主管者或管理者可要求固定通行碼與其他資訊或生物辨識掃描結合使用。

【0069】 使用者可經由聯絡主管者或管理者要求動態或固定的通行碼。舉例來說，使用者的行動裝置203可包括行動應用程式，其允許使用者透過行動裝置的行動數據(cellular data)連接、WiFi連接或NFC/藍芽連接寄送通行碼的請求給主管者裝置201、管理者裝置202或中心訪問伺服器205。另一個例子，使用者可經由打語音電話或從使用者行動裝置寄送文字訊息給主管者、管理者或中心訪問伺服器客服人員提交請求。以此方式，即使當時行動裝置無法連接網路或未裝有數據連接或網路連接，使用者仍可寄送請求。

【0070】 在本發明的一些實施例中，智慧鎖具204可藉由使用者提供的生物辨識掃描而打開。如下更詳細地描述，智慧鎖具204包括儲存媒體301，其可儲存授權訪問鎖具之各使用者的生物辨識數據。生物辨識數據例如可包括各使用者的指紋。當使用者接受生物辨識掃描時，智慧鎖具204比較該掃描和儲存在智慧鎖具204的生物辨識數據。若該掃描匹配儲存的生物辨識數據，智慧鎖具將授權使用者訪問。當生物辨識掃描器用於作為冗餘訪問通道時，若例如使用者不具有行動裝置或遺失行動裝置及獲得的許可證或通行碼無效，則使用者可提供生物辨識掃描。

【0071】 如第2C圖根據本發明的一些實施例繪示智慧鎖具204耦接至主管者裝置201、管理者裝置202或中心訪問伺服器206，從而略過行動裝置。舉例來說，智慧鎖具204可耦接至將通訊中繼給主管者裝置201、管理者裝置202或中心

訪問伺服器206的網路裝置217。網路裝置217可例如為無線接收器、路由器、中繼器等裝置。作為另一個例子，如下更詳細地描述，智慧鎖具204可透過行動寬頻網路連接直接與通訊給主管者裝置201、管理者裝置202或中心訪問伺服器206雙向通訊。

【0072】如第2C圖繪示，在智慧鎖具204與網路裝置217通訊的配置中，智慧鎖具204可使用近場無線傳送器或無線LAN以建立短程無線連接。該連接可使用例如藍芽、NFC、紫蜂(ZigBee)等的短程無線網路技術建立。舉例來說，網路裝置217可為裝置位於家裡的無線中繼器、延伸器或路由器，及使用藍芽與智慧鎖具通訊。接著，網路裝置217可使用網路連接，如網路、乙太網路等連接以耦接至主管者裝置、管理者裝置或中心訪問伺服器。接著，網路裝置217可接近即時地從智慧鎖具將該通訊中繼給主管者裝置、管理者裝置或中心訪問伺服器。因此，即使使用者的智慧手機或行動裝置被偷或不能運作，智慧鎖具仍可接近即時地與主管者裝置、管理者裝置或中心訪問伺服器通訊。

【0073】在本發明的一些實施例中，智慧鎖具可包括直接與中心伺服器或管理者通訊的無線發射器行動寬頻或廣域網路連接，以使鈕件直接與主管者裝置201、管理者裝置202或中心訪問伺服器206通訊。鎖具可包括用於創造行動寬頻連接且接近即時地通訊資訊的無線數據機。舉例來說，數據機可為嵌入在鎖具的晶片的Intel XMM 6255 3G 數據機。在更多的實施例中，數據機可為用於提供訪問行動網路之USB伺服器鑰、數據卡等裝置及可透過如下更詳細描述的輸入/輸出(I/O)埠耦接至鎖具。行動網路可例如為GSM/GPRS、EDGE、UMTS、HSDPA、HSPA、HSPA+、CDMA、LTE等的行動網路。

【0074】使智慧鎖具與主管者裝置、管理者裝置或中心訪問伺服器通訊，提供透過使用者訪問智慧鎖具的附加控制。舉例來說，智慧鎖具可配置成向主管者裝置或管理者裝置傳送請求，以用於核准每次使用者企圖獲得對智慧鎖具的訪問。因此，即使使用者嘗試使用通行碼或生物辨識掃描獲得訪問的情況下，主管者或管理者可核准各訪問的請求。

【0075】作為另一個例子，智慧鎖具可使用到主管者裝置、管理者裝置或中心訪問伺服器的連接以驗證被授權以打開智慧鎖具的使用者。具體而言，在接收認證資訊後，智慧鎖具可與主管者裝置、管理者裝置或中心訪問伺服器通訊，其核對一組可配置規則以驗證被授權訪問智慧鎖具的使用者。

【0076】在本發明的另一態樣中，主管者裝置、管理者裝置或中心訪問伺服器可通訊指示給智慧鎖具以執行某些功能或程序。舉例來說，若中心訪問伺服器確定智慧鎖具的門栓為解鎖時，中心伺服器可指示智慧鎖具鎖上門栓。以此方式，若管理者或使用者離開家而不記得是否有鎖門時，管理者或使用者可確認門是否未上鎖，若未上鎖則遠端鎖門。在其他實施例中，主管者裝置、管理者裝置或中心訪問伺服器可通訊指示給智慧鎖具以阻擋從某些裝置接收的通訊或從某些使用者接收的生物辨識。舉例來說，若已經報告使用者的行動裝置遺失或被偷，主管者裝置、管理者裝置或中心訪問伺服器可指示智慧鎖具阻擋從特定行動裝置接收的任何通訊。同樣地，主管者裝置、管理者裝置或中心訪問伺服器可寄送的指示給智慧鎖具，其不應再允許特定使用者使用他們的生物辨識掃描解鎖智慧鎖具及報告從該使用者接收的任何其生物辨識掃瞄。

【0077】根據本發明的一些實施例，鈕件包括慣性模組，以偵測及測量門的動作和位置。慣性模組可包括用於偵測及量測動作及/或位置的感測器的組

合，例如微機電系統(MEM)類型加速儀、陀螺儀及/或磁力計等。MEM類型加速儀可為單軸、雙軸或三軸加速儀及量測可例如包括透過該軸之門的速度及門的加速度。由加速儀提供的量測可進行過濾及分析以確定動作是否與開門或關門相關。可使用的其他感測器可包括磁性感測器，如產生對磁場改變的量測之電磁開關。電位計也可使用以產生對應於門框樞紐的角度運動及位置之訊號。其他實施例可包括量測隨著門開啟或關閉時的反射光或反射聲波之光學感測器或超音波感測器。

【0078】由慣性模組的感測器進行的量測可用於追蹤位置和門的動作的改變，以使鈕件確定門為開啟的或關上。在一些實施例中，鈕件可藉由比較感測器的量測與關於門的開關的已知加速度及/或動作曲線以確定門是否打開或關閉。舉例來說，關門的動作可以加速度的改變為特徵；若加速度急遽增加 (即，使用者推門)而接著突然減少(即，門接觸門框並關上)，則鈕件可確定門為關閉。作為另一個例子，關門的動作可以其速度為特徵；若速度或加速度到達最大臨界值，可確定門已經到達最終將使其關閉的速度或速率。同樣地，若門的速度或加速度未達到最小臨界值，可確定沒有以足夠關門的力推動門。鈕件可配置成持續追蹤打開門或關門的時間。舉例來說，鈕件可藉由保存在智慧鎖具的儲存媒體中的日誌記錄門何時被打開或關閉。

【0079】在本發明的進一步態樣中，這些感測器可使用於偵測鎖具鎖芯的門栓是否已經旋轉，從而表示使用者是否鎖門或未鎖門。舉例來說，加速計可使用於偵測導致門栓延伸進入門的榫眼之鈕件的轉動。鈕件也可配置成以持續追蹤凸輪部何時接合以鎖上或解鎖門栓。在一些實施例中，鈕件可整合門栓的鎖上或解鎖狀態以確認門是否打開或關上。舉例來說，若鈕件偵測門為關上，

鈕件可藉由確定門栓是否從解鎖狀態改變到鎖上狀態來確認門的關上，而表示門為關上且鎖住。

【0080】在本發明的一些實施例中，鈕件將門是否打開、關上、鎖住或解鎖傳輸給網路裝置、管理者裝置、主管者裝置或中心訪問伺服器。以此方式，使用者可遠端確定他們的門是否保持打開或關上。

【0081】第3A圖及第3B圖係根據本發明的一些實施例繪示智慧鎖具。智慧鎖具包括儲存媒體301、電源302、硬體處理器303、鎖芯304及鈕件305。智慧鎖具也可包括無線收發器306、通行碼鍵盤區307及生物辨識掃描器308。鎖芯包括接合門栓(未繪示)的凸輪部309。使用者提供認證資訊給智慧鎖具，其藉由硬體處理器303及儲存媒體301驗證。認證資訊可例如為使用者掃描指紋、輸入鍵盤區的通行碼或從使用者裝置無線傳輸的許可證。當智慧鎖具驗證認證資訊時，鈕件305接合凸輪部309而解鎖門栓。儲存媒體301儲存用於驗證認證資訊、維持訪問事件及智慧鎖具使用的日誌及識別智慧鎖具的資訊及數據。舉例來說，儲存媒體可儲存被認證以打開鎖具的使用者的生物辨識數據或識別智慧鎖具的獨特辨識符號。

【0082】硬體處理器303配置以根據主管者或管理者決定的訪問權及規則驗證從訪問通道接收的認證資訊。當使用者透過訪問通道認證時，硬體處理器可解鎖門栓。在本發明的一態樣中，當第一冗餘訪問通道對使用者為無效時，硬體處理器303配置成允許透過第二冗餘訪問通道訪問以解鎖門栓。

【0083】在一些實施例中，智慧鎖具包括用於傳輸及接收RFID、NFC或藍芽訊號給使用者行動裝置的無線收發器306。如上描述，使用者可無線傳輸許可證給智慧鎖具204。當無線收發器306接收許可證時，如上所述，智慧鎖具驗證

許可證。無線收發器也可將訪問資訊通訊給使用者行動裝置。訪問資訊詳細地提供關於訪問事件的資訊，如哪些使用者已經訪問智慧鎖具及其何時進行訪問。訪問資訊可儲存在智慧鎖具的儲存媒體301。訪問資訊儲存在智慧鎖具直到行動裝置訪問鎖具，此時智慧鎖具將傳輸訪問資訊給使用者的行動裝置。接著，行動裝置將訪問資訊通訊給中心訪問伺服器。當使用者的行動裝置被偷或無法接收無線通訊時，智慧鎖具將等待直到下一個可用的行動裝置企圖訪問智慧鎖具。

【0084】 智慧鎖具的鎖芯304可調整以符合門的標準外形插槽。在本發明的一些實施例中，智慧鎖具的鎖芯304係歐洲尺寸(或歐規(Euro DIN))設計。在其他實施例中，鎖芯可為橢圓類型、圓類型、斯堪地那維亞式(Scandinavian)、日式、合併式(Union)或施拉格式(Schlage)的外形。然而，歐規鎖芯通常包括在門的內側上且用於接合或脫離門栓之可旋轉旋鈕，替代智慧鎖具具有自由旋轉的鈕件305。與通常旋轉半圈或四分之一圈以接合或脫離門栓的旋鈕相比，自由旋轉的鈕件305可繞自軸旋轉多次。如下解釋的細節，旋轉的自由旋轉鈕件305產生旋轉能量，其可使用在供電及充電給門內側的電源302數天。

【0085】 當已經驗證使用者的認證資訊，智慧鎖具可接合鎖具。具體而言，鈕件305可向內推以啟動接合凸輪部309的傳動轉軸。當使用者持續轉動鈕件305，凸輪部309將門栓從鎖住位置移動到解鎖位置。使用者將無法打開智慧鎖具直到他或她已經被授權訪問位置(舉例來說，藉由無線傳輸許可證、提供生物辨識掃描或輸入通行碼在按鍵區)。直到使用者被授權，鈕件自由地旋轉，且將脫離凸輪部。

【0086】 如第3A圖繪示，設置鈕件在面向外側的鎖芯的一端。在本發明的一態樣，智慧鎖具使用單一鈕件，其讓智慧鎖具適用於不同的尺寸或鎖具規格。舉例來說，自由旋轉鈕件305也可適用於單一入口鎖具、鈕件入口鎖具、雙入口鎖具及掛鎖。掛鎖例如可只包括自由旋轉鈕件而不需內旋鈕。

【0087】 第3B圖根據本發明的一些實施例繪示鎖芯的前視圖。鈕件可包括許多訪問通道，如可由蓋部310隱藏的通行碼按鍵區307及生物辨識掃描器308。在使用者無法使用他們的行動裝置無線傳輸許可證解鎖鎖具的狀況(如，使用者的行動裝置被偷或裝置的電池耗盡)時，使用者可經由使用數字按鍵區輸入通行碼或使用生物辨識掃描而獲得訪問。當蓋部310在關閉位置時，蓋部310從視圖隱藏按鍵區307。

【0088】 如第3C圖繪示，智慧鎖具根據本發明的一些實施例包括設置在面向內側的鎖芯304的相反側的旋鈕或第二鈕件311。外側鈕件305可具有大於內側鈕件311之較長半徑及較大厚度，其如下更詳細地描述，其可減少需要轉動鈕件的力量或速度且可充電本身內部電源。在智慧鎖具包括內側鈕件311的實施例中，內側鈕件311可不需要提供認證資訊給智慧鎖具或從管理者或使用者要求訪問而可接合或脫離門栓。因此，使用者可在任何時間鎖住或解鎖門以離開地點的內部。

【0089】 根據本發明的一些實施例，鎖具可包括凸部保護件317及鈕件可形成如第3E圖所繪示的凸部旋鈕318。凸部旋鈕318保護及隱藏智慧鎖具內部的機械元件及電子元件，例如硬體處理器、電源及鎖芯等。同樣地，凸部保護件318保護及隱藏鎖具內部的機械元件及電子元件，例如硬體處理器、電源及鎖芯等。凸部保護件317及凸部旋鈕318同時包住內部機械元件及電子元件而因此徹

底地保護這些元件免於損害或攻擊。舉例來說，鑑於如上所述，對樞軸的強力擊打將嚴重損害或破壞鎖具內部的元件，凸部保護件317及凸部旋鈕318保護及避免如此破壞的動作。同樣地，凸部保護件317及凸部旋鈕318徹底地隱藏鎖芯以避免有人摘取鎖具。

【0090】如第3F圖繪示，凸部保護件317具有形成環狀槽321以用於與凸部旋鈕318互鎖之外壁319及內壁320。內壁320實質上相對於門322垂直地延伸。形成具有錐形的外壁319，其軸線實質上相對於門322垂直地延伸。由於外壁319的錐形形狀，環狀槽321具有沿垂直於門的面減少的漸變厚度。以此方式，外壁的錐形形狀偏轉撞擊在凸部保護件317之上的蠻力。舉例來說，有人使用鐵槌去敲擊凸部保護件317將由於錐形表面的曲率和角度而無法用鐵鎚的前端敲掉凸部保護件317。

【0091】凸部旋鈕318可具有外表面323及內表面324。外表面323及內表面324形成環狀邊緣325。環狀邊緣325形成為具有與環狀槽321的漸變厚度匹配的厚度，以讓環狀邊緣325與凸部保護件317的環狀槽321互鎖。外表面323及內表面324也形成開口326。內部機械元件及電子元件，例如電源、硬體處理器或用於接受認證資訊的冗餘訪問通道(如，生物辨識掃描器、通行碼按鍵區或無線收發器)可設置在開口326之內。

【0092】凸部旋鈕滑動地與凸部保護件317的環狀槽321契合而允許凸部旋鈕318繞著其中心軸自由地旋轉。根據本發明的一些實施例，凸部旋鈕318可自由轉動直到接收來自通行碼按鍵區、生物辨識掃描器或行動裝置的有效認證資訊。當已經提供有效的認證資訊時，如下所述，凸部旋鈕配置成啟動凸輪部以解鎖門栓。再者，如下更詳細地描述，當使用者無

法透過第一通道打開鎖具時，硬體處理器配置成允許透過第二通道訪問。以此方式，其他人無法意圖藉由施加粗暴的旋轉力破壞鎖具。亦即，鑑於一些鎖具可經由過度的旋轉力量旋轉鈕件而被破壞，凸部旋鈕318可自由地旋轉直到使用者提供有效的訪問資訊。

【0093】在本發明的一些實施例中，凸部旋鈕具有錐台336。接收生物辨識資訊的生物辨識掃描器308及通行碼按鍵區307都可設置於錐台336之上。生物辨識掃描器308可配置於錐台336的中心，及按鍵區307的按鍵可配置於生物辨識掃描器308的附近。以此方式，鎖具可同時提供多種訪問通道給使用者。

【0094】如第3G圖繪示，凸部保護件317可具有一組通孔327，其用於將凸部保護件固定於門的一個或多個固定桿328及一個或多個緊固件329。因此，當凸部旋鈕318的環狀邊緣325與凸部保護件317的環狀槽321滑動地互鎖時，凸部旋鈕318不可移動地固定於凸部保護件317。

【0095】在本發明的一些實施例中，鎖芯可為允許在各側的雙鈕件或雙按鍵訪問之雙入口鎖芯。此允許第一凸部保護件330及第一凸部旋鈕331設置於門332的一側上，而第二凸部保護件333及第二凸部旋鈕334設置於門332的相反側之上的實施例，如第3H圖繪示。在本發明的一些實施例中，電子元件及機械元件，例如硬體處理器及電源等可設置於由第一凸部旋鈕331及第二凸部旋鈕334形成的開口。在本發明更多的實施例中，其可為由兩個凸部旋鈕共享但設置於門的一側之上的單組電子元件及機械元件。舉例來說，在一些實施例中，其可為設置於第二凸部旋鈕334之內但亦耦接於第一凸部旋鈕331的單一硬體處理器或電源。較佳地，具有單組電子元

件及機械元件之凸部旋鈕係為設置於門332的內側上之上的凸部旋鈕。以此方式，若有人企圖破壞及損害外側凸部旋鈕，電子元件及機械元件將保持隱藏並保護在門的內側。

【0096】在本發明的一些實施例中，第二凸部保護件333可藉由一個或多個固定桿及一個或多個緊固件335固定於第一凸部保護件331。一個或多個緊固件可從第二凸部保護件333的門側插入。以此方式，一個或多個緊固件335被完全隱藏及從門的外側難以接近。因此，第一凸部保護件331無法移除，直到鬆開及移除第二凸部保護件333。

【0097】在本發明的一些態樣，凸部旋鈕318及凸部保護件317由堅固的材料構成，例如不鏽鋼等。以此方式，凸部旋鈕318及凸部保護件317可抵抗劇烈的力量。在本發明的部分實施例中，凸部旋鈕318及凸部保護件317的表面可由整理製程整理。舉例來說，凸部旋鈕318及凸部保護件317可由超音波拋光、磁性拋光、噴砂處理、振動、電鍍、化學塗佈、熱浸鍍(hot dipping)、拋光、研光(lapping)、研磨或磨光製程整理。這有助於預防其他人企圖如上所述施加過度的旋轉力量破壞或損害鎖具。根據本發明的一些實施例，整理製程或塗佈施加於表面以使表面平滑及實質上減少凸部旋鈕的摩擦係數。舉例來說，整理製程或塗佈可將鋼的摩擦係數從0.8減少到0.16或到0.04。減少的磨擦係數從而預防一些人施加旋轉力量而導致凸部旋鈕損壞。

【0098】雖然如機電鎖具描述的內容，根據本發明的進一步實施例，鈕件、凸部保護件317及凸部旋鈕318適合於包含各種類型、形狀及尺寸的智慧鎖具，例如機械鎖芯鎖具或掛鎖等。舉例來說，凸部保護件317及凸部旋鈕318可

用如上描述的單一入口圓筒鎖具之同樣的方式添加到掛鎖的鎖芯。作為另一個例子，鈕件、凸部旋鈕及凸部保護件可符合標準規格設計，例如歐洲設計(有時也稱為歐規鎖芯)、橢圓類型、圓類型、斯堪地那維亞式、日式、合併式或施拉格式(schlage)等的外形。在本發明的一態樣及優點中，凸部保護件317及凸部旋鈕318為模組且不需添加線或其他部件而可改裝成機械鎖具或掛鎖鎖芯的標準及/或先前存在的外形。因此，鈕件、凸部旋鈕及凸部保護件可使用於升級現存的鎖具及掛鎖而不需再加工門框、掛鎖連接環或掛鎖本體。以此方式，本發明可將任何鍵盤類型掛鎖或現今的機械鎖具實際地轉換成智慧無鍵鈕件類型掛鎖或鎖具系統(如，藉由添加鈕件、凸部保護件及凸部旋鈕至鎖芯而與本發明揭露的實施例一致)。

【0099】根據本發明的一些態樣，凸部旋鈕318進一步包括釋放機制，其允許將凸部旋鈕318向內壓以進一步旋轉動作。釋放機制可例如為設置在鈕件內側的一個或多個可移動的插銷或栓。如上所述，凸部旋鈕318可自由地轉動直到使用者提供有效認證資訊來啟動釋放機制。因此，直到使用者被認證，插銷或栓可設置在阻擋位置，以預防凸部旋鈕318被向內推動。一旦使用者被認證，插銷或栓從阻擋位置移動，以允許凸部旋鈕318被向內推動。一旦向內推動，凸部旋鈕318可接合鎖芯的門栓或門鎖(latch)。接著，凸部旋鈕318的進一步轉動可造成鎖芯門栓的打開或關閉 。

【0100】根據本發明的一些實施例，凸部旋鈕318啟動用於第一系列轉動的凸輪部，而在第一系列轉動之後，凸部旋鈕318可啟動鎖芯的門鎖。以此方式，凸部旋鈕318也可作為門把手的功能及使用於打開及關閉門鎖門栓。舉例來說，

第一系列的轉動可使用於接合或脫離鎖具門栓。接著，第二系列的轉動可使用於打開鎖具的門鎖，或若使用歐規鎖芯，該轉動將鎖上或解鎖鎖芯。

【0101】根據本發明的一些實施例，凸部旋鈕318的轉動動作也可以類似於可用於打開保險箱之旋轉數字鎖的方式作為密碼機制。凸部旋鈕可包括具有數字或文字許可證的顯示器。顯示器則可使用於讓凸部旋鈕318的旋轉動作與顯示器的數字或文字有關。因此，使用者可根據及參考這些標記以達到所需組合而藉由轉動凸部旋鈕提供動態通行碼或固定通行碼以打開鎖具。硬體處理器則可配置成基於以凸部旋鈕的旋轉動作與顯示器的數字或文字有關的凸部旋鈕的旋轉動作驗證認證資訊。硬體處理器接著可確定對應旋轉動作的通行碼，且接著如上下文所述的電子驗證通行碼。

【0102】第3D圖繪示在本發明的一些實施例中可從鎖芯拆離的鈕件。可拆離鈕件可包括充電介面313及輸入/輸出埠(「I/O埠」)314。電源302可為可充電電源，例如電容器組、可充電電池等裝置。如下更詳細地描述，鈕件也可包括能量收集元件316。藉由從鎖芯移除鈕件，使用者可將鈕件帶到可恢復充電的充電站315。充電站315可耦接至電源插座，其中，充電可經由充電介面313傳送至可充電電源302。充電介面313可例如為用於以匹配介面自充電站315接受電流之電線、插頭或一個或多個觸點接腳。當充電介面以匹配電線、插頭或觸點接腳配置耦接至充電站315時，充電站315供應電力給鈕件。可充電電源302儲存自充電站315接收的充電。

【0103】鈕件也可經由輸入/輸出埠314充電。輸入/輸出埠314可例如為USB、火線(Firewire)、雷電(Thunderbolt)、e-SATA、乙太網路或傳輸電力及/或數據的相似埠。在本發明的一些例子，輸入/輸出埠314可以傳輸電荷的匹配介面

而自外部裝置，如可攜式電池充電器接收電力。舉例來說，外部裝置可為具有USB連接之充電套組。在本發明的進一步實施例，輸入/輸出埠314可以匹配埠介面接收自充電站315的電力。充電站315可自電源插座經由輸入/輸出埠314傳輸電力到鈕件的電源302。

【0104】充電站315可耦接主管者裝置201、管理者裝置202或中心訪問伺服器206。舉例來說，充電站315可包括乙太網路埠或WiFi傳輸器，其用於建立網路連接及通訊給主管者裝置201、管理者裝置202或中心訪問伺服器206。當連接至輸入/輸出埠314時，充電站315可提取儲存在儲存媒體301的數據。如上描述，這些數據可例如包括驗證認證資訊、維持訪問資訊，如訪問事件及智慧鎖具使用之日誌、識別智慧鎖具的資訊及數據。充電站315則可寄送從儲存媒體301提取的數據到主管者裝置201、管理者裝置202或中心訪問伺服器206。因此，當鈕件在充電時，鈕件可通訊訪問資訊給其他裝置或中心訪問伺服器。

【0105】根據本發明的一些實施例，輸入/輸出埠314可使用於將智慧鎖具與無線數據機連接。舉例來說， USB伺服器鑰、數據卡或提供對行動網路訪問的相似裝置可插入至輸入/輸出埠，以使智慧鎖具透過行動寬頻連接通訊給主管者裝置、管理者裝置或中心訪問伺服器。

【0106】在本發明的一些實施例中，為了從鎖芯放出鈕件而需要有效資格。舉例來說，鈕件只可在接收到有效通行碼或生物辨識掃描時移除。以此方式，當鈕件設置於門的外側之上，鈕件不可被小偷或有害的破壞者移除或偷竊。在其他實施例中，鈕件可配置成從鎖芯移除而不需提供憑證。舉例來說，當鈕件設置於面向家的內側的門的內面上時，可在任何時間移除鈕件。

【0107】根據本發明的一些實施例，智慧鎖具包括設置於門的內面上的鈕件及設置於門的外面上的鈕件，如第3H圖繪示。在此配置中，設置於門的內面之上的鈕件係可移除及可充電的，而設置於門的外面之上的鈕件係不可拆離的及不可充電的。外側鈕件因此從內面鈕件的電源獲得電力。以此方式，可提供高效能的雙鈕件智慧鎖具且其具有抵抗外側損害的外側鈕件。

【0108】如上所述，經由行動裝置傳送的許可證可包括通行碼，如單次使用的動態通行碼。在本發明的一態樣中，通行碼可從行動裝置自動地通訊及產生而因此不需與使用者互動。具體而言，使用者行動裝置可確定或偵測其在智慧鎖具的附近。舉例來說，使用定位類型功能的行動裝置，行動裝置可確定使用者接近的地點。在一些實施例中，該確定可經由分析過去使用者模式來幫助，及推斷使用者從工作回家及是在其路上打開他們的家門。行動裝置可經由使用NFC/藍芽或無線功能替代的進行此確定。直到偵測鎖具，行動裝置可辨認鎖具及鎖具固定的地點。行動裝置則可自動通訊此資訊給中心訪問伺服器以確定是否允許使用者訪問智慧鎖具。若使用者滿足訪問鎖具的所有條件(如，允許使用者在特定時間及特定日期訪問鎖具)，則訪問控制系統將產生動態通行碼。動態通行碼可產生在主管者裝置、管理者裝置或中心訪問伺服器，且隨後傳輸動態通行碼到行動裝置，或替代地由使用者的行動裝置的行動應用程式產生動態通行碼。行動裝置接著可傳輸通行碼到智慧鎖具，其使用儲存在鎖具的程序驗證通行碼。一旦驗證通行碼，使用者可把鈕件向內推及使用傳動轉軸系統接合或脫離門栓。若不允許使用者打開鎖具，管理者將接收未被授權的使用者企圖打開鎖具的通知。

【0109】根據本發明的一些實施例，鈕件包括根據操作模式改變顏色的光指示器312。舉例來說，若接受認證資訊，則發出綠光；若拒絕認證資訊，則發出紅光；若在等待模式，則發出藍光。

【0110】如上所述，智慧鎖具由電源302供電。在本發明的一些實施例，鈕件包括冗餘電源，如第4圖所繪示。在其中一個電源故障的情況下，冗餘電源可使用於供電儲存媒體、無線收發器及光指示器。冗餘電源可例如為位在鈕件的內側的電容器組或電池組401。當電池或電容器係在低電荷時，鈕件可通訊此資訊給下一個訪問鎖具的行動裝置。行動裝置則可通訊此資訊給主管者或管理者。或者，可使用顏色指示器通訊低電荷或低電池電平。

【0111】在其他實施例中，鈕件具有藉由鈕件的旋轉動作充電的電容器組。經由旋轉動作儲存的電力足夠持續幾天，及當另一個電力供應源(如電池)故障，其提供方便、可靠及冗餘的電源。鈕件繞其中心軸自由地轉動以產生高水平的動能。雖然一些旋鈕被限制在四分之一圈或二分之一圈，但鈕件可旋轉整圈。類似於手錶上的錶冠的纏繞，鈕件的旋轉動作被收集且經由鈕件內側的元件轉換成電能，且儲存電能作未來使用。鈕件旋轉的轉數越大，越多的電荷儲存在鎖具內側。在一個例示性實施例，鈕件的旋轉動作驅動一系列的齒輪及彈簧402，其轉換由轉動鈕件產生的旋轉能量。因為在鎖具內側的彈簧及齒輪402可小於鈕件，因此可以低速及低力矩旋轉鈕件。因此，供電鎖具的力量可藉由適當比例地調整鈕件與鎖具內側的齒輪及彈簧的尺寸而減少。

【0112】在其他實施例中，鈕件的旋轉動作施加在壓電元件403。當使用者轉動鈕件時，鈕件的旋轉動作施加於壓電元件而產生壓電 (piezoelectricity)，其轉換成電荷並儲存在電容器組或電池組。壓電效應可藉由鈕件轉動之應力、

張力、扭力產生。應力、張力、扭力施加在壓電元件及產生可儲存在電容器組的電荷。在其他實施例中，壓電可藉由轉換旋轉動作為振動能而產生。具體而言，鈕件內側的齒輪或彈簧可接觸壓電振片(piezo flap)，其因鈕件的每個轉動而振動。

【0113】在其他實施例中，旋轉動作可另外轉換成靜電能或電磁能。舉例來說，鈕件的旋轉可使用作為機械能，其在電子產生器404內轉動電樞(armature)。在更多實施例中，鈕件的旋轉動作可儲存在彈簧等的機械裝置。

【0114】雖然第3A圖到第3C圖及第4圖描述鈕件內側的許多元件，在本發明的其他實施例中，這些元件可設置於鈕件的外側。舉例來說，無線收發器、記憶體、硬體處理器及電池組/電容器組可設置於鎖具殼的鎖芯及鈕件的外側。這些元件可透過鎖芯耦接鈕件。在其他實施例中，這些元件可位於鎖芯核心的內側或門凸部的內側。

【0115】第5圖根據本發明的實施例繪示使用具有訪問通道之鎖具的程序。在步驟501，使用者選擇第一訪問通道。若通道如步驟502繪示係可用時，使用者可提供認證資訊504。舉例來說，若訪問通道為無線傳輸許可證到智慧鎖具時，例如當使用者行動裝置遺失、遭偷竊或耗盡時，可決定訪問通道為無效。若第一訪問通道係為無效，接著選擇第二冗餘訪問通道503。舉例來說，第二冗餘訪問通道可為生物辨識掃描或輸入在智慧鎖具的按鍵區的通行碼。

【0116】智慧鎖具如步驟505繪示驗證認證資訊。如上描述，若認證資訊包括許可證或通行碼，比較許可證或通行碼和儲存在智慧鎖具的程序產生的許可證或通行碼。若認證資訊為生物辨識掃描，則比較掃描數據與儲存在智慧鎖具

的生物辨識數據。以此方式，本發明提供冗餘訪問通道以確保使用者即使在其行動裝置遺失或不可操作時仍可訪問鎖具。

【0117】若驗證認證資訊，則可確認訪問權以確定是否授權使用者訪問智慧鎖具，如步驟506繪示。舉例來說，其確定主管者或管理者是否允許使用者在特定日期或特定時間訪問智慧鎖具。若使用者被授權打開智慧鎖具，則同意使用者訪問及鈕件可接合凸輪部以打開智慧鎖具507。若認證資訊係無效的，或管理者或主管者決定拒絕使用者訪問鎖具，鈕件將不接合凸輪部及不打開智慧鎖具508。如上描述，可在使用者裝置、中心訪問伺服器、主管者裝置或管理者裝置中確認規則及訪問權。

【0118】第6圖根據本發明的實施例繪示控制具有訪問通道的鎖具之程序。在步驟601中，登記觸發事件。觸發事件可使用以啟動自動開始打開智慧鎖具的程序。觸發事件可例如為使用者的行動裝置進入與智慧鎖具的預定距離(如10英尺)內時。觸發事件則可例如造成行動裝置自動傳輸許可證到鈕件。

【0119】觸發事件可根據行動裝置的其他功能登記。舉例來說，若行動裝置具有手勢辨認感應器及軟體，觸發事件可為根據當使用者用特定方式搖動其行動裝置而登記。或者，當使用選擇鈕件或輸入通行碼在行動裝置的行動應用程式上時，行動裝置可登記觸發事件。

【0120】行動裝置登記觸發事件後，行動裝置識別其打開的智慧鎖具，如步驟602繪示。接著，其確定規則是否配置成同意使用者條件式訪問權或固定訪問權，如步驟603繪示。若使用者具有條件式訪問權，則行動裝置將如步驟604繪示提交請求給主管者或管理者。否則，在步驟605中，評估規則及訪問權以確定是否授權使用者打開智慧鎖具。

【0121】如上描述，行動裝置可用許多方式提交請求給管理者。舉例來說，使用者可使用數據連接以寄送文字訊息或藉由打電話給客服中心的中心訪問伺服器提交請求給主管者裝置、管理者裝置或中心伺服器。在本發明的一些實施例中，主管者、管理者或中心訪問伺服器可在發布許可證前要求使用者提供額外的憑證。舉例來說，由使用者行動裝置提交的請求可包括使用者位置、密碼或其他相似辨視憑證，如他們的手機號碼或電子郵件住址。作為另一個例子，額外的憑證可包括使用者行動裝置的全球定位系統(GPS)座標，以證實使用者在智慧鎖具的位置。在其他實施例中，也可要求使用者拍攝智慧鎖具的相片及向其提供請求以證實使用者位在智慧鎖具的位置。在成功地驗證憑證後，寄送許可證到使用者的行動裝置。

【0122】若主管者或管理者核准使用者的請求，或使用者有足夠訪問權打開鎖具，則使用者可如步驟606繪示接受許可證。若主管者或管理者拒絕使用者的請求，或未授權使用者打開鎖具，使用者將無法如步驟607繪示接收許可證。

【0123】使用者接著可如步驟608繪示提供認證資訊給智慧鎖具。若使用者藉由輸入通行碼在按鍵區將打開鎖具，使用者例如可接受使用者可輸入在智慧鎖具按鍵區之文字訊息的通行碼或顯示在行動應用程式的通行碼。若使用者行動裝置無線傳輸許可證到智慧鎖具，則一旦接收到許可證，行動裝置可自動地傳輸許可證。

【0124】在本發明的一態樣中，在可提供認證資訊到智慧鎖具之前，可需要額外的安全層。舉例來說，在行動裝置將無線傳輸認證資訊到鈕件前，可提示使用者輸入密碼在行動裝置。在其他實施例中，規則可配置成在接受許可證前，要求使用者掃描其指紋在行動裝置上。如上所述，行動裝置也可自動地傳

送認證資訊而不需與使用者進一步互動。舉例來說，行動裝置可在啟動行動應用程式時傳輸認證資訊。

【0125】 在一些實施例中，鈕件可為裝置的內連集線器(inter-connected hub)的部分，其可以單一介面控制並且可根據發生在訪問控制系統的事件而自動化。舉例來說，裝置的內連網路可包括透過WiFi或藍芽無線通訊的家庭恆溫器、照明系統、聲音系統及訪問控制系統。家庭恆溫器、照明系統、聲音系統及訪問控制系統可使用相同應用程式介面(Application Programming Interface，API)互相通訊或與中心伺服器通訊。使用應用程式介面，家庭恆溫器、照明系統、聲音系統及訪問控制系統可根據某些規則或事件而自動化。舉例來說，使用者用他的行動裝置解鎖家門之後，訪問控制系統可通訊使用者偏好至恆溫器以在特定溫度下打開空調、在客廳打開部分光源裝置及透過揚聲器系統開始播放使用者自訂的特定音樂。

【0126】 在一些實施例中，如上所述之門的移動或位置可登記觸發事件而使裝置的內連集線器執行特定工作或任務序列。舉例來說，當確定門已經打開時，觸發事件可登記以通訊給恆溫器以在特定溫度下打開空調、在客廳打開部分照明裝置及透過揚聲器系統開始播放使用者自訂的特定音樂。

【0127】 第6圖繪示主管者或管理者可控制訪問控制系統的程序。在步驟701，顯示一組配置規則及訪問權給主管者或管理者。在步驟702，主管者或管理者配置訪問權以決定使用者可訪問哪個智慧鎖具。在步驟703，主管者或管理者配置規則，其指定使用者可使用哪個訪問通道打開智慧鎖具及(若需要時)在使用者打開鎖具前需滿足何種條件。

【0128】當具有條件式訪問權的使用者如上所述提交請求以打開智慧鎖具時，主管者或管理者接收訪問請求，如步驟704繪示。舉例來說，請求可以文字訊息、電話呼叫或在主管者或管理者的行動應用程式中顯示的通知的形式接收。請求可直接從使用者接收，或可從接收使用者請求的中心訪問伺服器接收。

【0129】在步驟705中，驗證使用者請求。可藉由例如請求使用者提供額外的憑證，如密碼驗證使用者。作為另一個例子，主管者或管理者可獲得使用者行動裝置的ID以確定行動裝置是否已經報告為遺失或被偷竊。若行動裝置被偷竊，規則可配置成自動拒絕訪問請求及通知主管者、管理者或企圖使用的使用者。

【0130】若主管者或管理者驗證使用者，則主管者或管理者可進行至步驟706，其中，主管者或管理者決定是否同意使用者的訪問。在這個步驟中，可確認規則及訪問權以決定使用者是否被授權打開特定鎖具及在打開鎖具前是否需滿足任何條件。舉例來說，可決定不授權使用者打開特定智慧鎖具或在特定日期不授權使用者打開智慧鎖具。若授權使用者，主管者或管理者仍可決定拒絕使用者的訪問。舉例來說，即使授權使用者，主管者或管理者可偏好使用其判斷力同意請求。若主管者或管理者決定同意請求，則產生許可證或通行碼且提供給使用者。許可證或通行碼可如上所述傳輸給使用者。舉例來說，許可證或通行碼可以文字訊息、電話呼叫形式或在使用者的行動應用程式中顯示的通知形式寄出。接著，在步驟708，許可證或通行碼可提供給使用者。

【0131】根據本發明的一些實施例，行動應用程式可安裝在主管者裝置、管理者裝置或使用者裝置以控制訪問控制系統的使用。主管者或管理者的行動應用程式可提供介面以：查看訪問資訊；建立訪問權；查看訪問日誌；管理使

用者權；打開鎖具；及建立成功進入的報告及拒絕進入的報告，其包括為何拒絕進入的細節(例如，使用者在允許訪問鎖具的時間框架或日期以外訪問鎖具，或在第一例子中不允許打開鎖具)。以此方式，訪問控制系統提供機械鎖具及鑰匙系統的安全性及可靠性效益，同時也提供行動裝置及電子鎖具系統的報告及即時增值服務(real-time value-added services)。同樣地，用於使用者的行動應用程式可提供介面以：接收訪問警告；請求訪問權；查看訪問日誌；及打開鎖具。

【0132】在本發明的一態樣中，行動應用程式提供如第8A圖繪示的「通知者」特徵，其告知主管者、管理者及使用者關於訪問事件及訪問權的資訊。對於主管者及管理者，行動應用程式將接收關於訪問事件的資訊，如當使用者訪問鎖具。如第8A圖繪示，此特徵提供警告給主管者或管理者，約翰・史密斯(Johnson Smith)欲打開大門、接近大門或企圖打開大門。警告接近即時地通知主管者或管理者訪問事件或改變訪問權。因為可迅速通訊事件給主管者或管理者，行動應用程式可額外提供主管者或管理者選項以接近即時地拒絕使用者訪問安全地點。同樣地，當使用者企圖用無效認證資訊打開鎖具(如，不正確的通行碼)，行動應用程式也可接收警告。

【0133】使用行動裝置的無線功能或定位類型功能，行動應用程式可決定使用者待在安全地點的時間長度。行動應用程式也可從鈕件接收關於何時鎖上或打開鎖具的資訊以確定使用者何時獲得訪問及隨後何時離開安全地點。如下更詳細地解釋，鎖具上的鈕件亦將傳輸其鎖上/解鎖狀態給使用者的行動裝置。使用者的行動裝置可接著傳輸鎖上/解鎖狀態給中心訪問伺服器，其可接著傳送關於鎖具狀態之通知給使用者或管理者。以此方式，使用者隨後離開安全地點

後，可警告主管者或管理者地點仍為解鎖，及其可聯絡使用者以告知其忘記鎖上地點。

【0134】在本發明的一態樣，行動應用程式可顯示給主管者或管理者已經鎖住或解鎖哪些安全地點的區域，如第8B圖繪示。當使用者用他們的行動裝置鎖上或解鎖地點時，行動裝置通訊此資訊給中心訪問伺服器。中心訪問伺服器則可提供鎖上/解鎖狀態給主管者或管理者。當使用者使用替代的訪問通道鎖上或解鎖地點時，儲存資訊在智慧鎖具且下次使用行動裝置打開智慧鎖具時傳送給中心訪問伺服器。

【0135】行動應用程式也程式化以提供用於顯示及配置如何可解鎖這些地點的使用者介面。舉例來說，如第8C圖繪示，行動應用程式可顯示地點是否可自動打開或手動打開。

【0136】行動應用程式的另一個介面提供哪些使用者已經訪問鎖具的顯示。如第8D圖繪示，介面顯示各使用者的照片及他們的個人資訊，如名字和聯絡資訊。可選擇或刪除在表單上的各使用者。選擇的使用者可使行動應用程式顯示另一個介面，其顯示關於使用者的額外詳細資訊。

【0137】本發明的一態樣中，通知者將顯示關於對使用者訪問權進行改變之警告及訊息。如第8E圖繪示，通知者可警告使用者其在特定時間(例如，從星期一到星期五的5:00pm到8:00pm)具有特定地點(如，大門A)的訪問權。同樣地，通知者可通知使用者其接收到特定區域的新訪問權或已經被限制或撤除的訪問權。

【0138】雖然第8A圖到第8E圖顯示使用行動應用程式介面的通告者之警告功能及訊息功能，但關於訪問權的警告及訊息也可經由SMS文字、電子郵件

或電話呼叫傳送給使用者。因此，舉例來說，當使用者的訪問權改變時，使用者可接收告知使用者其訪問權已改變的SMS文字。

【0139】在本發明的一態樣，行動應用程式提供「授權(authorization)」特徵，其可使主管者及管理者建立及改變使用者的訪問權，並且允許使用者請求訪問權。各使用者的訪問權儲存在主管者裝置、管理者裝置或中心訪問伺服器，其中可驗證嘗試訪問鎖具的各使用者。

【0140】如第9A圖繪示，行動應用程式可主管者或管理者提供介面以建立使用者的訪問權及規則。舉例來說，介面允許主管者或管理者規定使用者聯絡資訊(如，名字、電話號碼、職業、年紀)、使用者將具有訪問的特定個別鎖具、使用者可使用的訪問通道(如，通行碼、生物辨識掃描、無線傳輸許可證至智慧鎖具或其任意組合)及使用者訪問的條件(如，限制在某天的時間)。行動應用程式的授權特徵對於主管者及管理者為可用的。在由管理者使用授權特徵的一些實施例中，在提供訪問資訊後，管理者提交資訊作為請求的資訊給主管者。接著，資訊可傳送給主管者，其最終同意或拒絕新使用者的訪問權之建立。訪問權的建立可接近即時地發生；當主管者同意使用者請求或管理者請求時，使用者可立即開始使用他們的行動裝置、通行碼或生物辨識掃描以訪問指定的智慧鎖具。

【0141】在本發明的一態樣，主管者或管理者可指定特定鎖具、區域或地點的門，如第9B圖繪示。如第9B圖繪示，主管者或管理者可選擇鎖住區域，如前門、健身房、娛樂間或辦公室以同意使用者的訪問。行動應用程式可使此配置遠端且接近即時地發生；主管者或管理者不需在地點進行備分鑰匙或更新任何紀錄而造成延遲。

【0142】狀態可對應從如上所述的感應器接收的資訊，其對應門的打開或關閉及門栓的鎖住或解鎖。

【0143】如上所述，授權特徵允許主管者或管理者增加對使用者訪問的限制。如第9C圖繪示，主管者或管理者可允許使用者具有無限永久訪問或可將使用者訪問限制成暫時性或可將訪問限制在整個日、週、月或年的選擇區間期間。

【0144】授權特徵可額外允許主管者或管理者在個別基礎上提供一次性訪問。使用者可藉由如上所述寄出請求給主管者或管理者而接收一次性訪問。請求可為透過使用者的行動應用程式授權介面的SMS文字、電子郵件或藉由電話呼叫。請求可用於特定鎖具或鎖具群，以及用於特定訪問類型。主管者或管理者可接近即時地決定同意或拒絕請求。若主管者或管理者同意請求，使用者可打開鎖具。使用紀錄及報告功能，主管者或管理員可確定使用者何時完成使用鎖具，及禁止或移除使用者的訪問權。或者，若主管者或管理員決定同意使用者的訪問，主管者或管理員可提供只可使用一次的動態通行碼給使用者，及在使用之後失效。

【0145】如第9D圖繪示的訪問類型介面允許主管者或管理者配置規則以指定何種訪問通道可供使用者打開智慧鎖具。舉例來說，主管者或管理者可指定使用者是否可藉由無線傳輸許可證給智慧鎖具、輸入通行碼在按鍵區、使用生物辨識掃描或其任意組合而打開智慧鎖具。主管者或管理者也可添加條件以限制使用者何時可訪問智慧鎖具，如添加時間限制或日期限制。舉例來說，主管者或管理者可指定使用者可在星期一到星期五用智慧手機或行動裝置訪問鎖具，但在週末時必須額外提供生物辨識掃描或通行碼。

【0146】在本發明的一個實施例中，主管者或管理者可使用其各別的行動裝置添加使用者生物辨識掃描到智慧鎖具。舉例來說，使用者可掃描他們的指紋到其智慧手機，並且經由SMS文字或行動應用程式寄送到主管者或管理者。接著，主管者或管理者可將指紋添加到中心訪問伺服器，或下次主管者或管理者的行動裝置與智慧鎖具通訊時給智慧鎖具。以此方式，新使用者的生物辨識掃描可遠端添加到智慧鎖具而不需使用者事先位在智慧鎖具。

【0147】使用者可使用行動裝置的行動應用程式寄出對訪問權的請求。登記之後，使用者可載入地點的清單及其對應的鎖具及從對應主管者或管理者的智慧鎖具的訪問請求。使用者可搜尋主管者或管理者及直接自其請求訪問權。作為使用行動應用程式之替代，使用者可藉由SMS文字、電子郵件或電話呼叫而請求訪問。

【0148】主管者或管理者可在任意時間經由授權介面修改各使用者的訪問權，如第9E圖繪示。在本發明的一態樣，可不需通知或告知使用者而修改訪問權。以此方式，主管者或管理者可遠端改變或刪除關於行動裝置的訪問權而不需任何訪問或與使用者互動。因此，若行動裝置被偷竊或遺失，主管者或管理者可使特定行動裝置失效，以避免未授權的人或以不期望的方式使用。在行動裝置可被失效之前，可提示主管者或管理者要求額外憑證以辨識其身分。若失效的智慧手機接著使用於訪問智慧鎖具(如，由小偷或不期望的人)，智慧鎖具將會拒絕它及在將通知主管者或管理者未授權者嘗試訪問。如下列例示性圖式繪示，授權介面允許主管者或管理者對使用者解除授權(de-authorize users)、使用者失效或完全從鎖具將其移除。針對使用者訪問權的改變可為接近及時地發生。

【0149】在本發明的一態樣，行動應用程式提供「報告(reporting)」特徵，其可使主管者及管理者查看各使用者或各鎖具的訪問事件的紀錄或日誌。如使用者何時及如何尋求或獲得智慧鎖具的訪問之各種訪問事件的紀錄可儲存在如上所述鈕件的儲存媒體或在使用者行動裝置的行動應用程式。舉例來說，當使用者使用其行動裝置尋求或獲得智慧鎖具的訪問時，訪問事件的紀錄可儲存在行動裝置中或在鈕件中。同樣地，若使用者經由冗餘訪問通道(如，通行碼或生物辨識掃描)訪問智慧鎖具，訪問事件可儲存在鈕件中，且在當另一個行動裝置與智慧鎖具接觸時的後期階段，將無線通訊給中心訪問伺服器。

【0150】訪問事件可進一步包括藉由如上所述的感測器接收的資訊指出門是否已經關閉或打開，或門栓已經鎖上或解鎖。

【0151】各使用者或各智慧鎖具的訪問事件日誌可接近即時或定期地編輯並通訊給主管者或管理者。舉例來說，如第9F圖繪示，可編輯某天的使用者的訪問事件的日誌並報告給主管者或管理者。日誌顯示特定使用者的各訪問事件的細節，如訪問哪個智慧鎖具、如何進行訪問及使用者訪問的精確時間及使用者在地點待了多久。日誌可進一步包括成功地及未成功打開智慧鎖具、允許使用者打開智慧鎖具的時段及使用者何時請求訪問智慧鎖具的紀錄。可對各智慧鎖具編輯相似的日誌，並報告何者訪問智慧鎖具、如何進行訪問及何時進行訪問。主管者或管理者可配置其偏好接收日誌報告之頻率。報告可傳送給中心訪問伺服器或直接傳送給主管者或管理者。

【0152】在本發明的其他實施例中，日誌可直接從智慧鎖具經由行動裝置直接通訊給管理者或中心訪問伺服器。如上所述，智慧鎖具可使用本身的無線連接或透過網路裝置直接將此資訊傳送給中心伺服器或管理者。

【0153】 在本發明的一態樣中，可處理日誌及報告以發現關於訪問使用及使用者的模式。具體而言，可探勘日誌及報告以偵測關於使用者如何及何時訪問不同智慧鎖具的模式。使用這些訪問行為的確認模式，訪問控制系統接著預測訪問事件，以增強系統安全或訪問控制。舉例來說，若日誌及報告指出使用者在平日5:00pm從前門進入家裡，訪問控制系統可使內連裝置中的程序或任務自動化，如通訊給照明系統以啟動在前露台的照明，通訊給恆溫器打開空調。

【0154】 第10圖的10A到10C部分繪示用於記錄在行動應用程式、要求許可證或通行碼及接收許可證或通行碼之使用者介面。如上所述，在允許請求通行碼或許可證之前，如10A部分繪示，可要求使用者提供憑證，如通行碼。如10B部分，介面允許使用者查看其可訪問的智慧鎖具，及若使用者無法訪問智慧鎖具，或只具有條件式訪問權，他們可提交請求給主管者或管理者。如10B部分繪示，使用者可以各種方式提交請求，例如經由寄送警告給主管者或管理者的行動裝置上的行動應用程式、或藉由寄送文字或打電話等。如10C部分繪示，若使用者由主管者或管理者驗證且同意訪問，使用者將接收許可證或通行碼。若使用者接受到通行碼，將可顯示用於使用者的通行碼輸入在按鍵區。若使用者接收許可證，許可證可無線傳輸給智慧鎖具。

【0155】 在本發明的更多態樣，以日誌發現的使用者模式可用以最佳化智慧鎖具的部分元件。舉例來說，日誌可使用於確定使用者通常何時離開及抵達家。藉由此資訊，智慧鎖具可確定智慧鎖具最不可能使用的部分期間，及因此可改變智慧鎖具的部分功能或操作模式。舉例來說，智慧鎖具可確定在平日的工作時間通常沒有人進入或離開家。在此期間，智慧鎖具可進入「睡眠」模式，其中智慧鎖具不啟動部些特徵以減少能量耗損。

【0156】所屬技術領域中具有通常知識者可進行本文所述內容的變化、修改及其他實施方式而不悖離本發明及其申請專利範圍的精神及範圍。

【符號說明】

【0157】

100：鎖具

101：機電型鎖芯

102：金屬棒

103~105：電子裝置

106、304：鎖芯

108、305：鈕件

109：門框

110：使用者裝置

111：防鑽孔凸部

112：旋入

200：訪問控制系統

201：主管者裝置

202：管理者裝置

203：使用者裝置

204：智慧鎖具

205：中心訪問伺服器

206：遠端伺服器

207：螢幕顯示器

208：儲存媒體

209：處理器

210、306：無線收發器

211：NFC元件

212：規則

213：訪問權

214：生物辨識掃描

215：按鍵區

216：行動裝置

217：網路裝置

301：儲存媒體

302：電源

303：硬體處理器

307：通行碼按鍵區

308：生物辨識掃描器

309：凸輪部

310：蓋部

311：內側鈕件

312：光指示器

313：充電介面

314：輸入/輸出埠

315：充電站

316：能量收集元件

317：凸部保護件

318：凸部旋鈕

319：外壁

320：內壁

321：環狀槽

322、332：門

323：外表面

324：內表面

325：環狀邊緣

326：開口

327：通孔

328：固定桿

329、335：緊固件

336：錐台

330：第一凸部保護件

331：第一凸部旋鈕

333：第二凸部保護件

334：第二凸部旋鈕

401：電池組

402：齒輪

403：壓電元件

404：電子產生器

501~508、601~608、701~707：步驟

【發明申請專利範圍】

【第1項】一種用於提供訪問的冗餘通道之鎖具，其包含：

一硬體處理器；

一電源；

一鎖芯，為可調式以符合一門的標準外形插槽，該鎖芯包括接合一門栓的一凸輪部；

一鈕件，係用於接合該凸輪部以解鎖該門栓並且用於形成保護及隱藏該硬體處理器、該電源及該鎖芯之一凸部旋鈕；以及

一凸部保護件，係用於保護及隱藏該硬體處理器、該電源及該鎖芯，使得該硬體處理器、該電源及該鎖芯藉由該凸部旋鈕及該凸部保護件整體地保護及隱藏，

其中，該凸部保護件具有一外壁及一內壁，而該外壁及該內壁形成一環狀槽以與該凸部旋鈕互鎖，其中，該內壁相對於該門而實質上垂直地形成，該外壁相對於該門而錐形地形成，該環形槽由於該外壁的錐形形狀而具有沿著垂直於該門的一平面減少的一漸變厚度，其中該外壁的形狀偏轉蠻力的撞擊，

其中，該凸部旋鈕具有一外表面及一內表面，該外表面及該內表面形成：1)一環狀邊緣，其用於與該凸部保護件的環狀槽互鎖，該環狀邊緣具有與該環狀槽的該漸變厚度匹配的厚度；以及 2)一開口，其包括該電源、該硬體處理器及用於接收認證資訊的複數個冗餘訪問通道，該冗餘訪問通道包括用於接收生物辨識資訊的一生物辨識掃描器、一通行碼按鍵區以及配置成與一行動裝置接近即時地通訊的一無線收發器，

其中，該凸部保護件具有一組通孔，其用於將該凸部保護件固定於該門的一或多個固定桿及一或多個緊固件，並且當該凸部旋鈕的環狀邊緣與該凸部保護件的環狀槽滑動地互鎖時，該凸部旋鈕為不可移動地固定於該凸部保護件，

其中，該凸部旋鈕為自由地旋轉直到自該通行碼按鍵區、該生物辨識掃描器或該行動裝置接收有效的認證資訊，此時該凸部旋鈕配置成啟動該凸輪部以解鎖該門栓，以及

其中，該硬體處理器配置成基於由一管理者決定的一組規則有效化自該通行碼按鍵區、該生物辨識掃描器或該行動裝置接收的認證資訊，當一使用者透過該複數個冗餘訪問通道的一第一通道認證時，解鎖該門栓，以及當該使用者無法透過該第一通道打開該鎖具時，允許透過該複數個冗餘訪問通道的一第二通道進行訪問。

【第2項】 如申請專利範圍第 1 項所述之鎖具，其中該鎖芯係為允許從兩側輸入訪問的雙入口鎖芯，其中該硬體處理器係為一第一硬體處理器，該電源係為一第一電源，該凸部保護件係為一第一凸部保護件，及該凸部旋鈕係為一第一凸部旋鈕，該鎖具進一步包括：

一第二硬體處理器；

一第二電源；

一第二鈕件，係用於接合該凸輪部以解鎖該門栓並且用於形成保護及隱藏該第二硬體處理器、該第二電源及該鎖芯之一第二凸部旋鈕，

一第二凸部保護件，係用於保護及隱藏該第二硬體處理器、該

第二電源及該鎖芯，使得該第二硬體處理器、該第二電源及該鎖芯藉由該第二凸部旋鈕及該第二凸部保護件整體地保護及隱藏；以及

其中，該第二凸部保護件具有一外壁及一內壁，而該外壁及該內壁形成一環狀槽以與該第二凸部旋鈕互鎖，該內壁相對於該門而實質上垂直地形成，該外壁相對於該門而錐形地形成，該環形槽由於該外壁的錐形形狀而具有沿著垂直於該門的一平面減少的一漸變厚度，其中該外壁的形狀偏轉蠻力的撞擊，

其中，該第二凸部旋鈕具有一外表面及一內表面，該外表面及該內表面形成：1)一環狀邊緣，其用於與該第二凸部保護件的環狀槽互鎖，該環狀邊緣具有與該環狀槽的該漸變厚度匹配的厚度；以及 2)一開口，包括該第二電源及該第二硬體處理器，

其中，該第二凸部保護件具有一組通孔，其用於將該凸部保護件固定於該門的一或多個固定桿及一或多個緊固件，並且當該第二凸部旋鈕的環狀邊緣與該第二凸部保護件的環狀槽滑動地互鎖時，該第二凸部旋鈕為不可移動地固定於該第二凸部保護件，以及

其中，該第一凸部保護件及該第一凸部旋鈕係設置於該門之外部上，且該第二凸部保護件及該第二凸部旋鈕係設置於該門之內部上。

【第3項】如申請專利範圍第 2 項所述之鎖具，其中該第二凸部保護件藉由一或多個固定桿或一或多個緊固件固定於該第一凸部保護件，其中該一或多個緊固件係從該第二凸部保護件插入，並且由該門的外部側隱藏。

【第4項】如申請專利範圍第 1 項所述之鎖具，其中該凸部旋鈕具有一錐台，以及其中用於接收生物辨識資訊的該生物辨識掃描器及該通行碼按鍵區係設置於該錐台之上。

【第5項】如申請專利範圍第 1 項所述之鎖具，其中該凸部旋鈕及該凸部保護件係由不銹鋼構成。

【第6項】如申請專利範圍第 1 項所述之鎖具，其中該凸部旋鈕具有一平滑表面，該平滑表面具有實質上減少該凸部旋鈕的摩擦係數的塗佈。

【第7項】如申請專利範圍第 1 項所述之鎖具，其中該鎖具係從機電鎖、機械鎖及掛鎖組成之群組中選出。

【第8項】如申請專利範圍第 1 項所述之鎖具，其中該凸部旋鈕係基於驗證認證資訊而藉由啟動從一阻擋位置移動到一非阻擋位置，使該凸部旋鈕向內推並基於進一步旋轉而接合該凸輪部的釋放機制來啟動該凸輪部以解鎖該門栓。

【第9項】如申請專利範圍第 1 項所述之鎖具，其中該凸部旋鈕啟動該凸輪部的第一系列轉動，及在啟動該第一系列轉動之後，啟動該鎖芯的門鎖。

【第10項】如申請專利範圍第 1 項所述之鎖具，其進一步包括該凸部旋鈕的旋轉動作與一文數顯示器相關之一數字顯示器，及其中該硬體處理器進一步配置成基於該凸部旋鈕的旋轉動作驗證認證資訊，其中該凸部旋鈕的旋轉動作與該文數顯示器相關並且對應於一通行碼，以及其中該硬體處理器電子地驗證該通行碼。

【第11項】一種提供冗餘訪問通道的訪問控制系統，其包括：

如申請專利範圍第 1 項所述之鎖具；

一使用者行動裝置，係配置成請求對該鎖具的訪問；

一管理者裝置，係用於控制該使用者行動裝置對該鎖具的訪問，該管理者裝置係配置成接近即時地同意或拒絕訪問的請求，其中基於同意對該鎖具的訪問，該使用者行動裝置係配置成接收包括打開該鎖具的一許可證之認證資訊，並且提供該許可證給該鎖具；以及

其中，該鎖具包括用於一儲存訪問資訊的一儲存媒體，及該鎖具係配置成傳輸包括該儲存訪問資訊的一回應。

【第12項】如申請專利範圍第 11 項所述之系統，其中從該鎖具傳輸的該回應包括指出該鎖具是否接受該許可證及打開該鎖具的訪問紀錄，及其中傳輸該回應的步驟包括將該回應接近即時地自該使用者行動裝置傳輸到該管理者裝置。

【第13項】如申請專利範圍第 11 項所述之系統，其中該管理者裝置係配置成基於一組配置規則同意該使用者裝置的訪問，以及其中該一組配置規則包括：

一使用者角色，係與對一或多個鎖具的一組允許相關，該一組配置規則係基於使用者的位置、訪問該鎖具的時間及該使用者角色來限制使用者的訪問；以及

一觸發事件，該行動裝置係基於該行動裝置登記的該觸發事件而自動地寄出訪問該鎖具的請求。

【第14項】如申請專利範圍第 11 項所述之系統，其中該電源係為可充電電源且包括一壓電元件，以及一鈕件的旋轉動作施加在該壓電元件並產生儲存在該可充電電源的壓電。

【第15項】如申請專利範圍第 1 項所述之鎖具，其中該無線收發器進一步

配置成接近即時地與 1)一網路裝置、2)一控制訪問伺服器及 3)一管理者裝置的其中之一通訊。

【第16項】如申請專利範圍第 15 項所述之鎖具，其進一步包括一無線數據機，係配置成建立一行動寬頻連接及接近即時地與該管理者裝置或一中心訪問伺服器通訊，並且建立一短程無線連接以接近即時地與該管理者裝置或該中心訪問伺服器通訊。

【第17項】如申請專利範圍第 16 項所述之鎖具，其中該鎖具係配置成基於使用者的生物辨識掃描、通行碼或行動裝置 IMEI 接收透過該行動寬頻連接自該中心訪問伺服器或該管理者裝置的一指示以阻擋使用者的訪問。

【第18項】如申請專利範圍第 16 項所述之鎖具，其中該鎖具係配置成：

接收一許可證、一生物辨識掃描或一通行碼，

基於一組配置規則傳輸對該鎖具訪問的請求，以及

自該管理者裝置或該中心訪問伺服器接近即時地接收同意或拒絕的訪問請求的一指示。

【第19項】如申請專利範圍第 16 項所述之鎖具，其中，該鈕件包括配置以確定門的狀態之一慣性模組，其表示該門是否開啟或關閉，並且接近即時地將該門的狀態傳送至該管理者裝置或該中心訪問伺服器，且其中該鎖具係配置成確定一門栓狀態，其表示該門栓是否位於鎖住位置或解鎖位置，以及接近即時地將該門栓狀態傳送至該管理者裝置或該中心訪問伺服器。

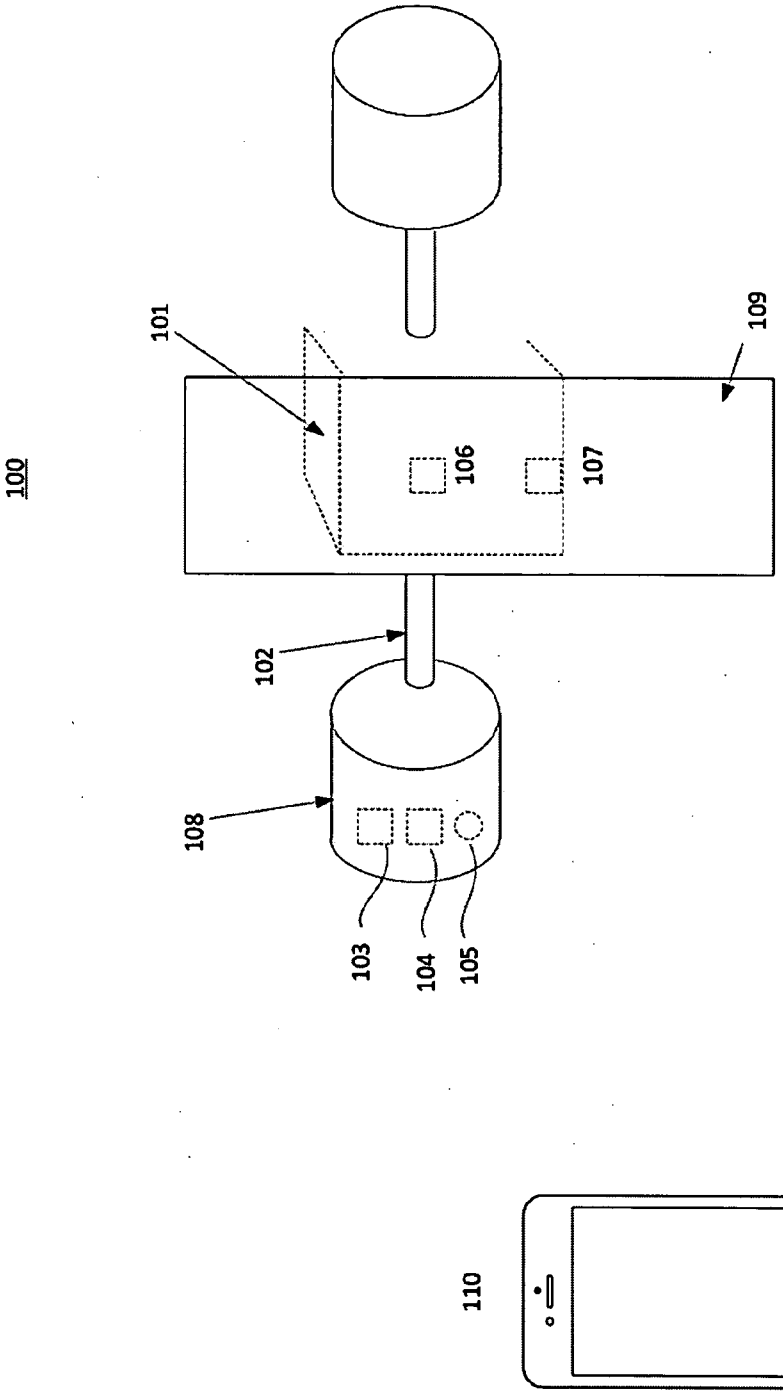
【第20項】一種用於控制具有冗餘訪問通道的鎖具之系統，該系統包括：

如申請專利範圍第16項所述之用於提供冗餘訪問通道的鎖具；

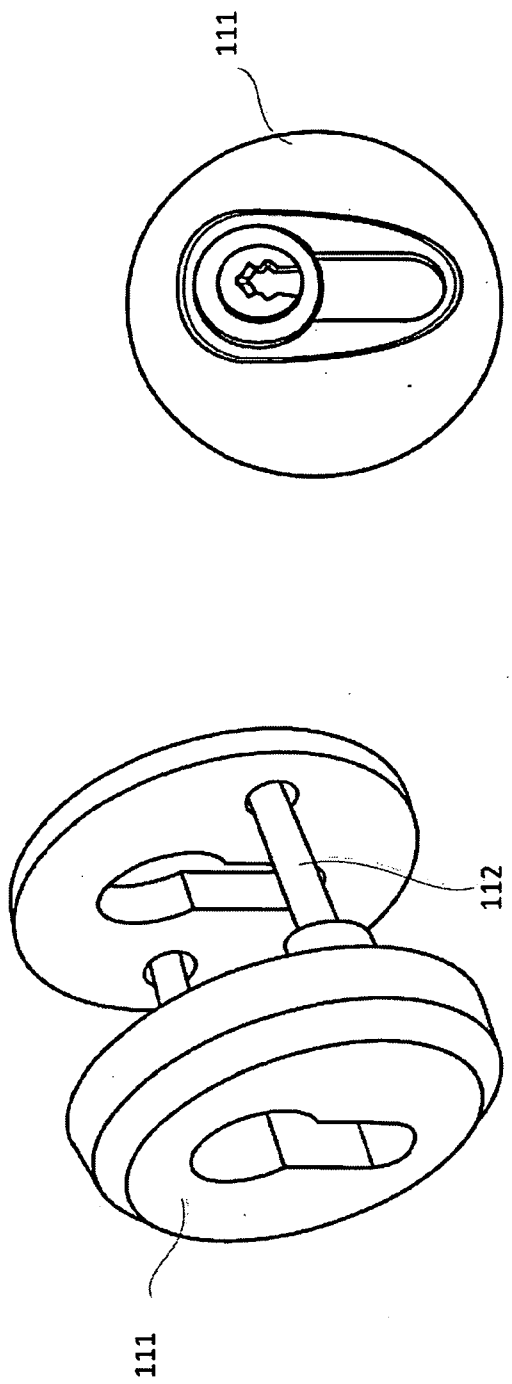
以及

一網路裝置，其中該鎖具透過一短程無線連接耦接到該網路裝置，以及該網路裝置透過一網路連接耦接到該管理者裝置或該中心訪問伺服器。

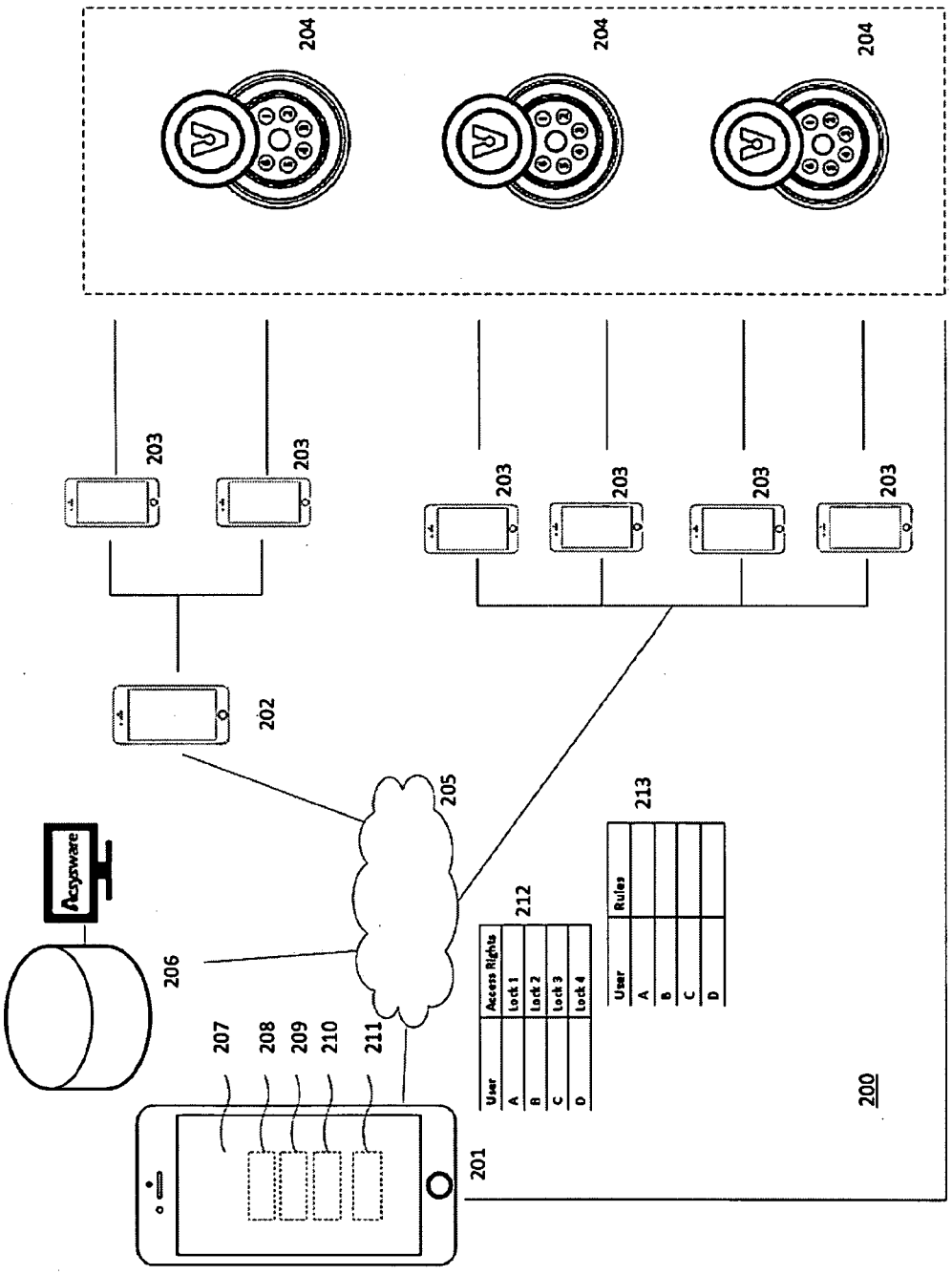
【發明圖式】



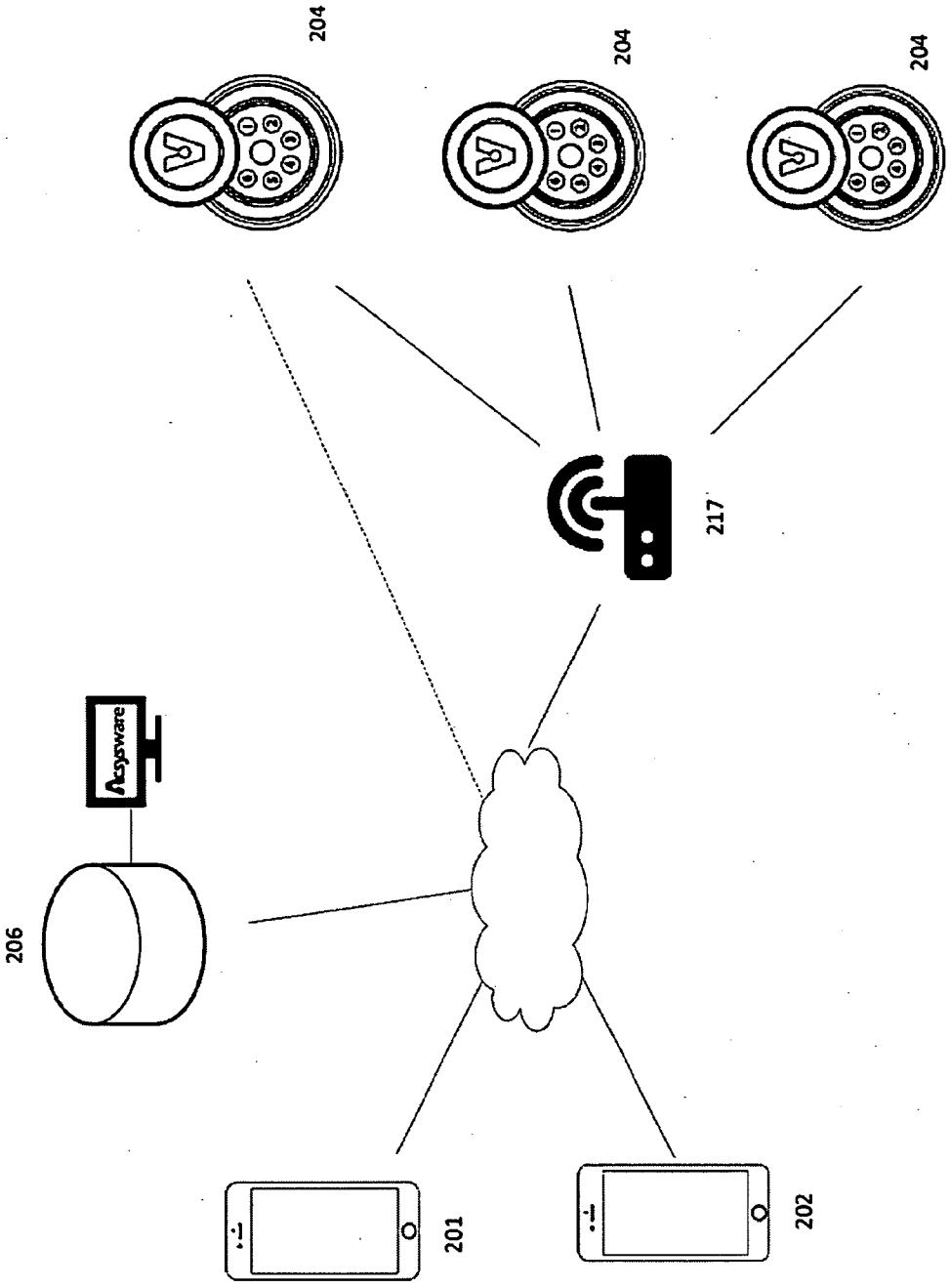
第 1A 圖



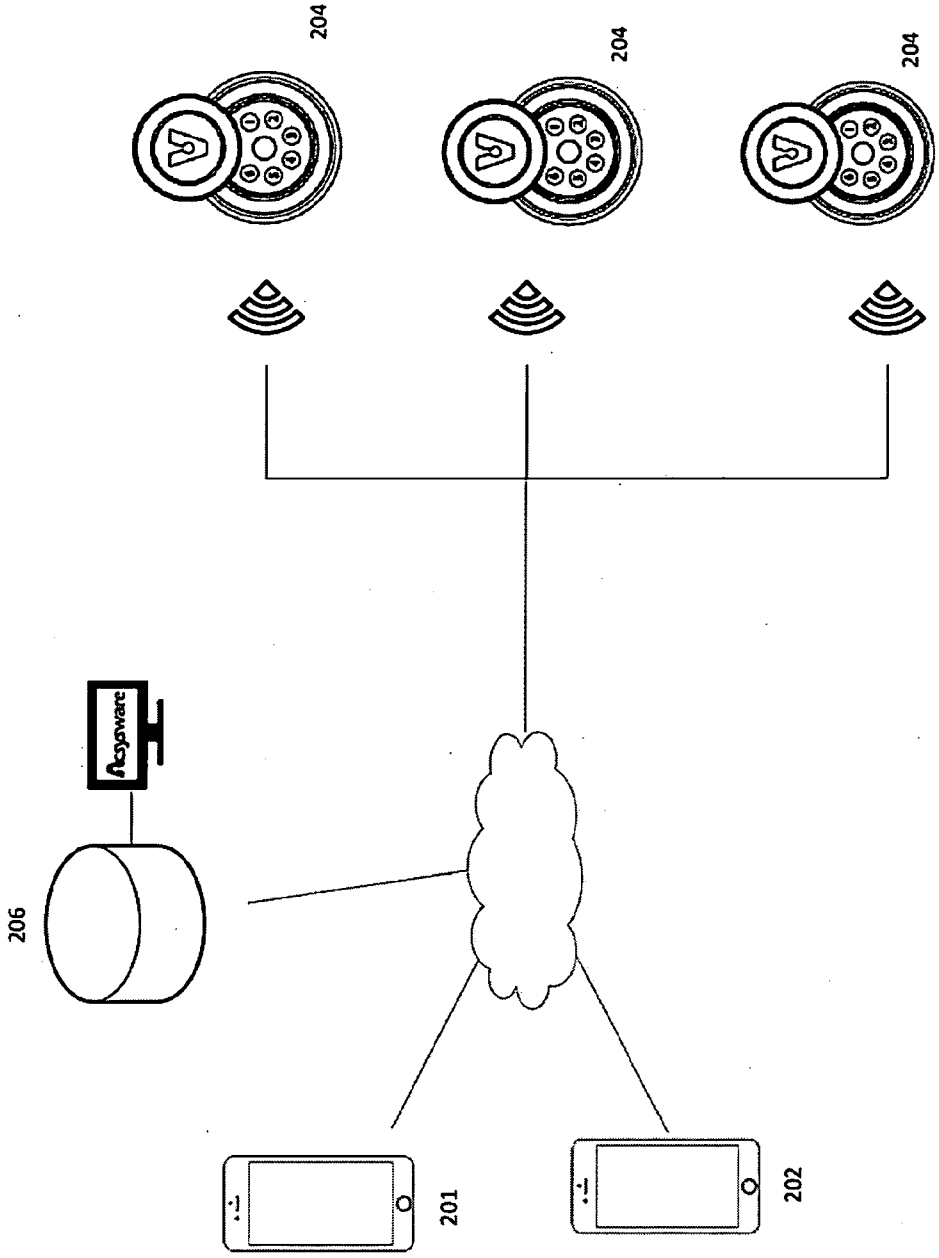
第 1B 圖


204
204
204
203
203
203
203
203
203
202
205
213
212
206
207
208
209
210
211
200
201
Rules
User
A
B
C
D
Access Rights
Lock 1
Lock 2
Lock 3
Lock 4

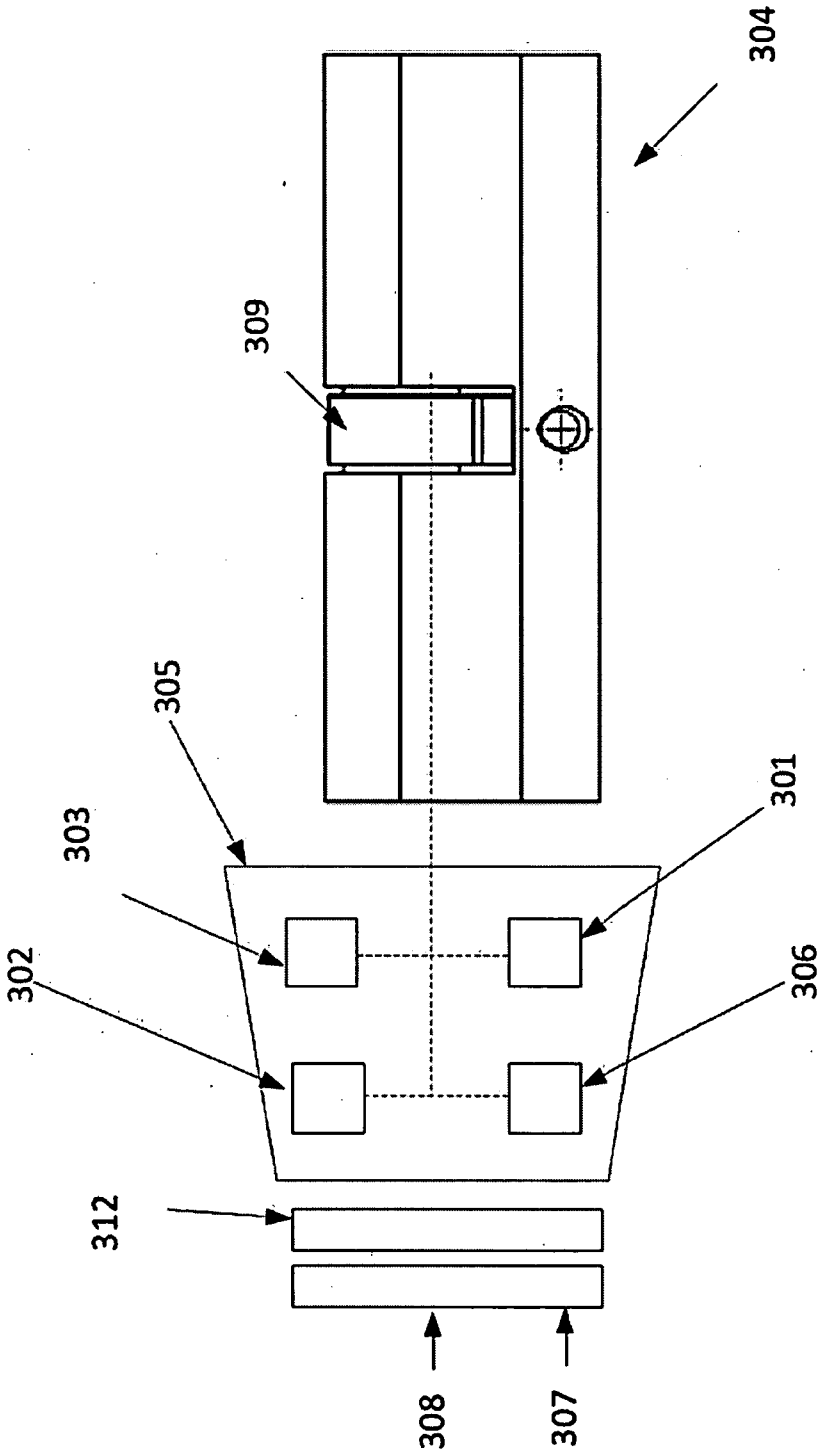
第 2A 圖



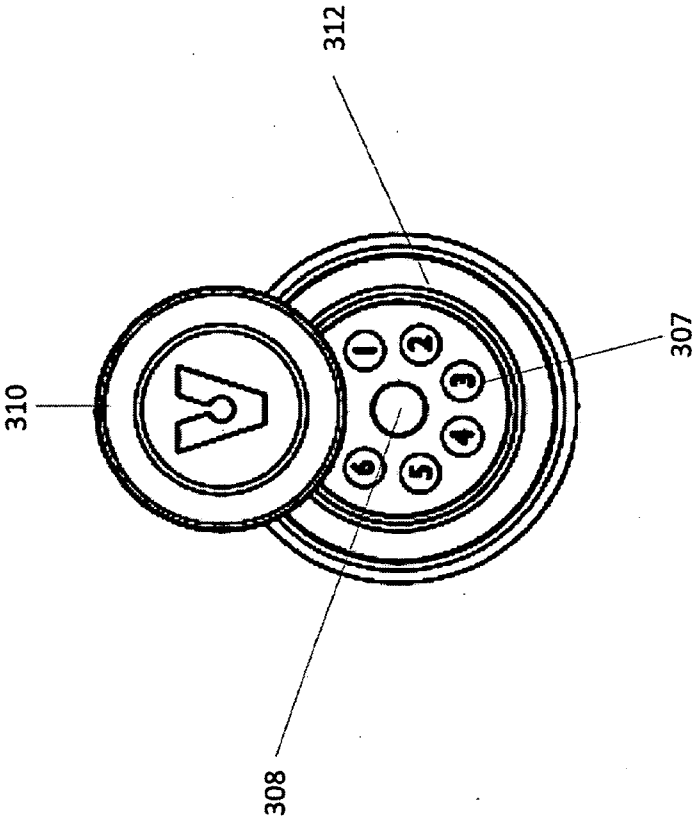
第 2C 圖



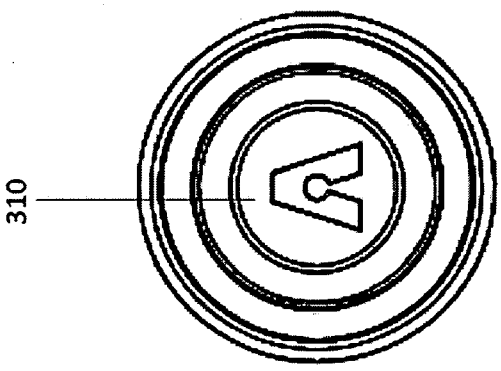
第 2D 圖

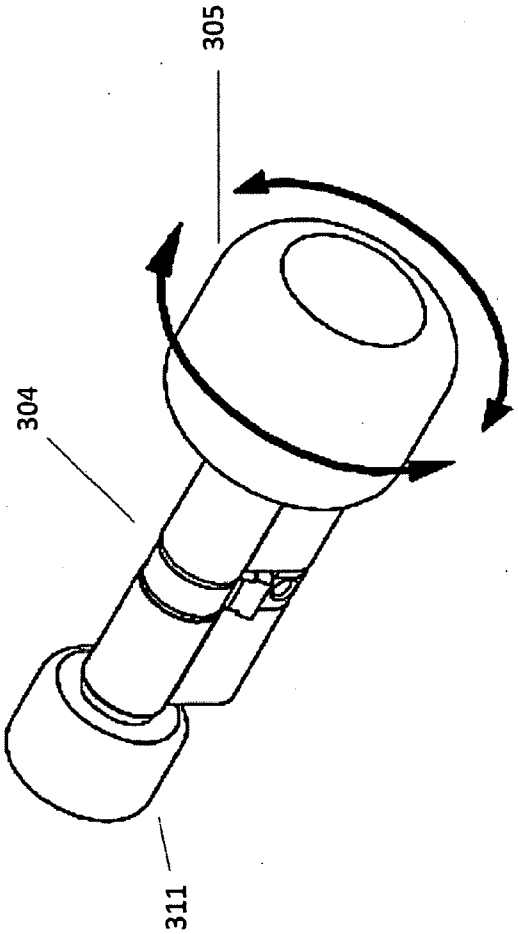


第 3A 圖

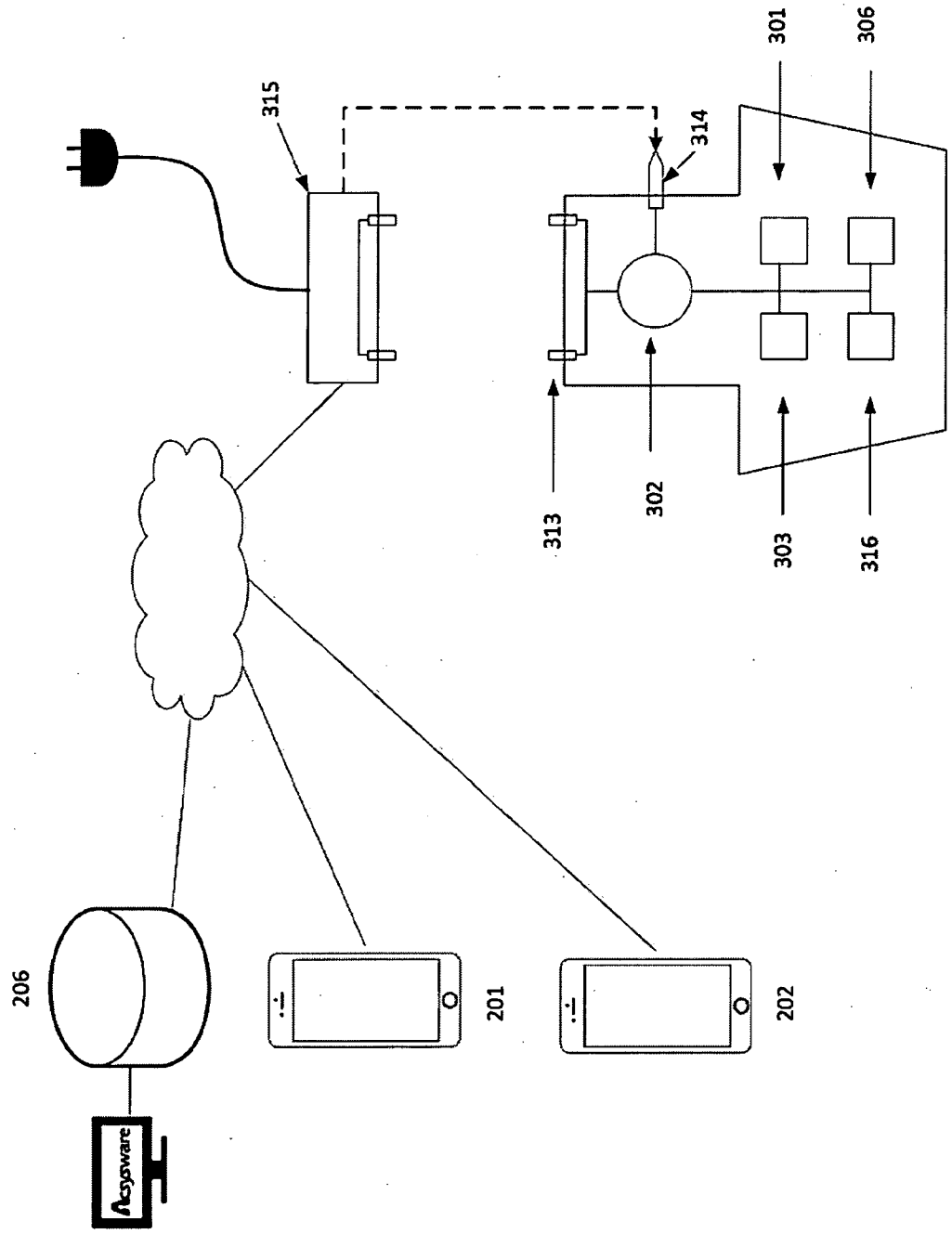


第 3B 圖

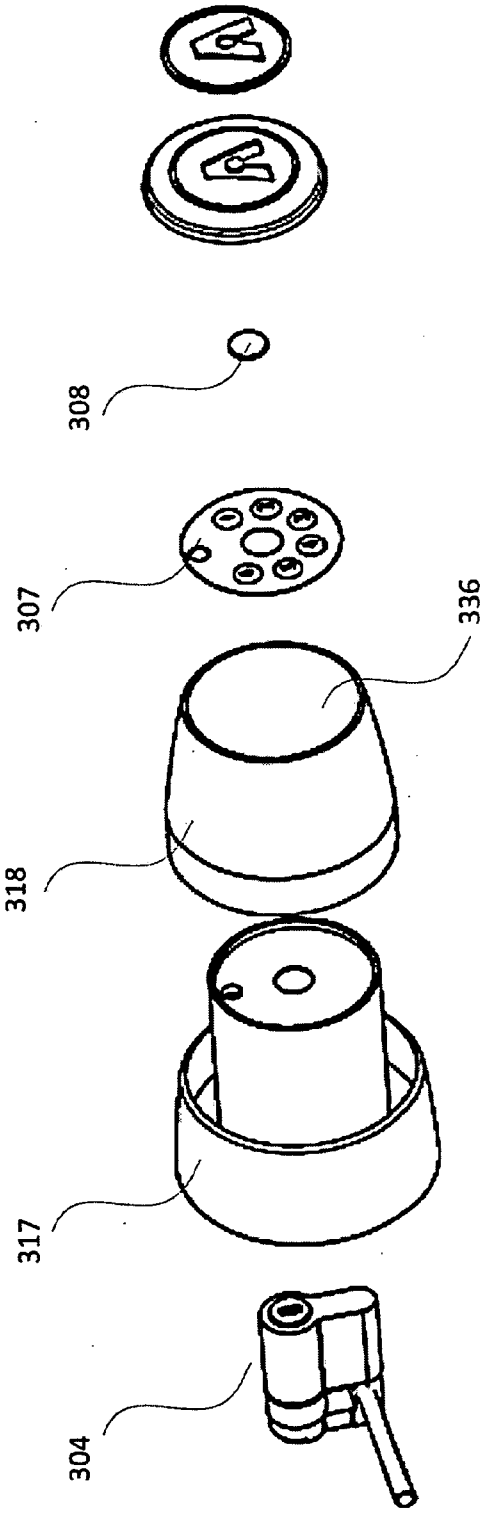




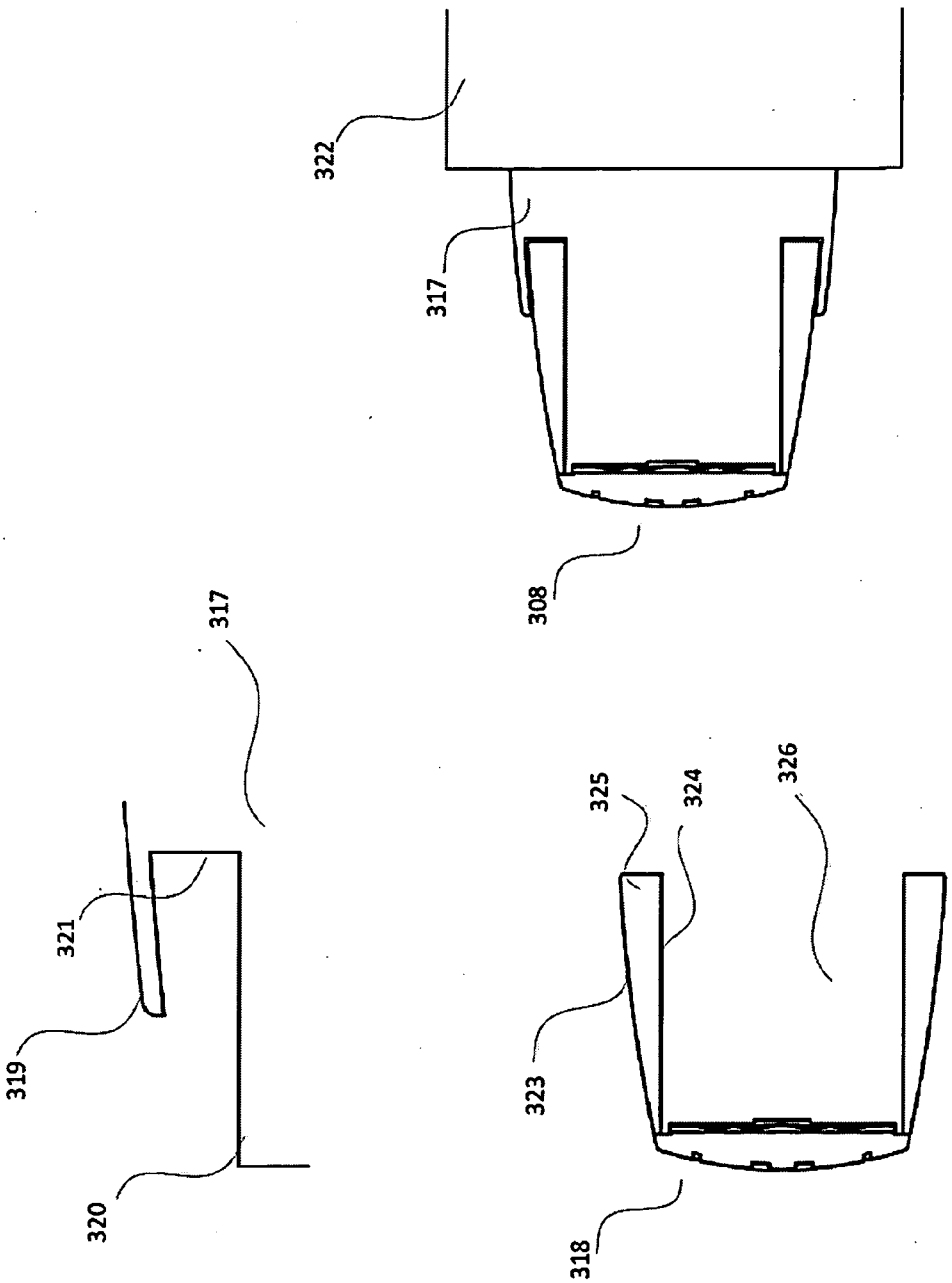
第 3C 圖



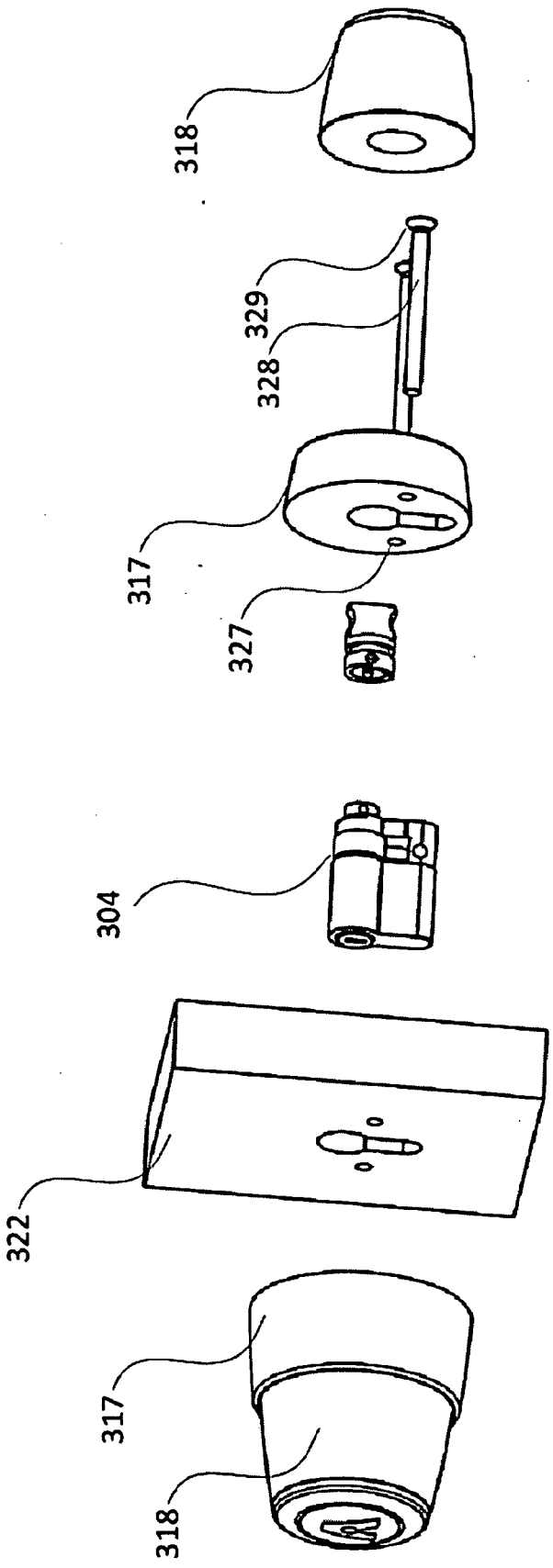
第 3D 圖



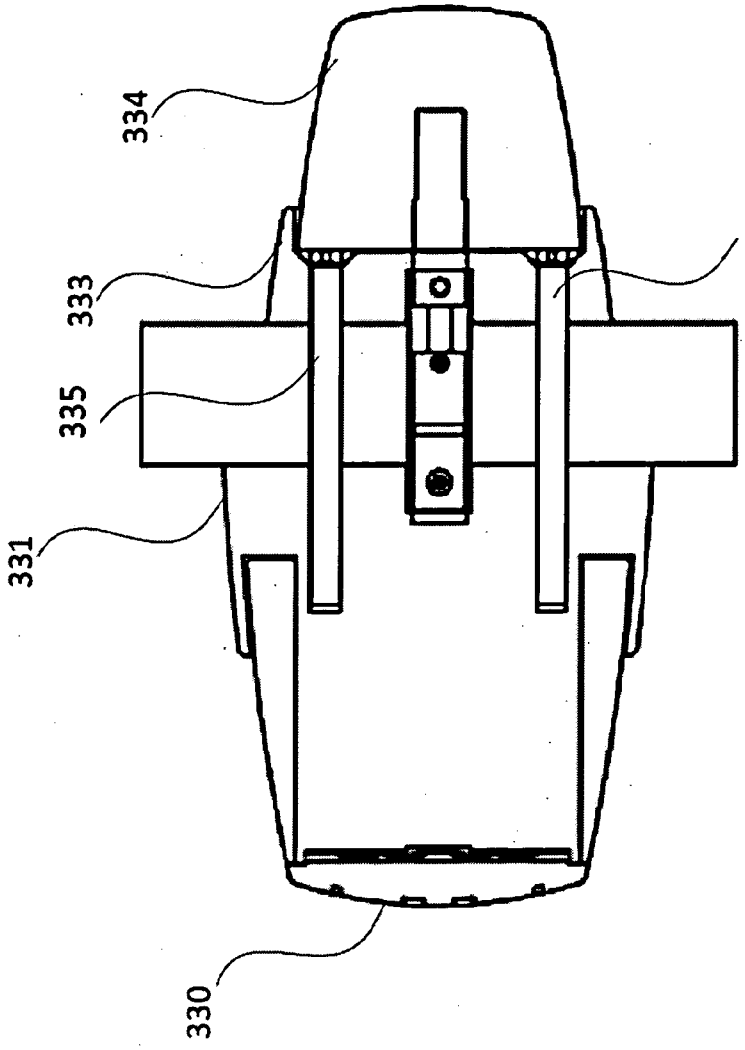
第 3E 圖



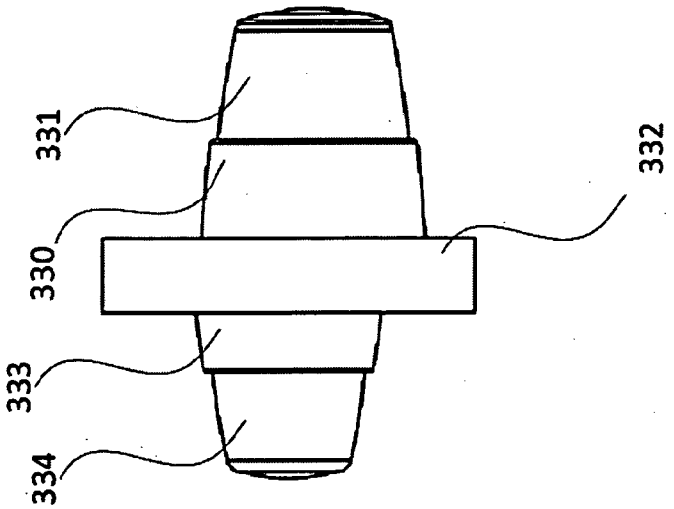
第 3F 圖

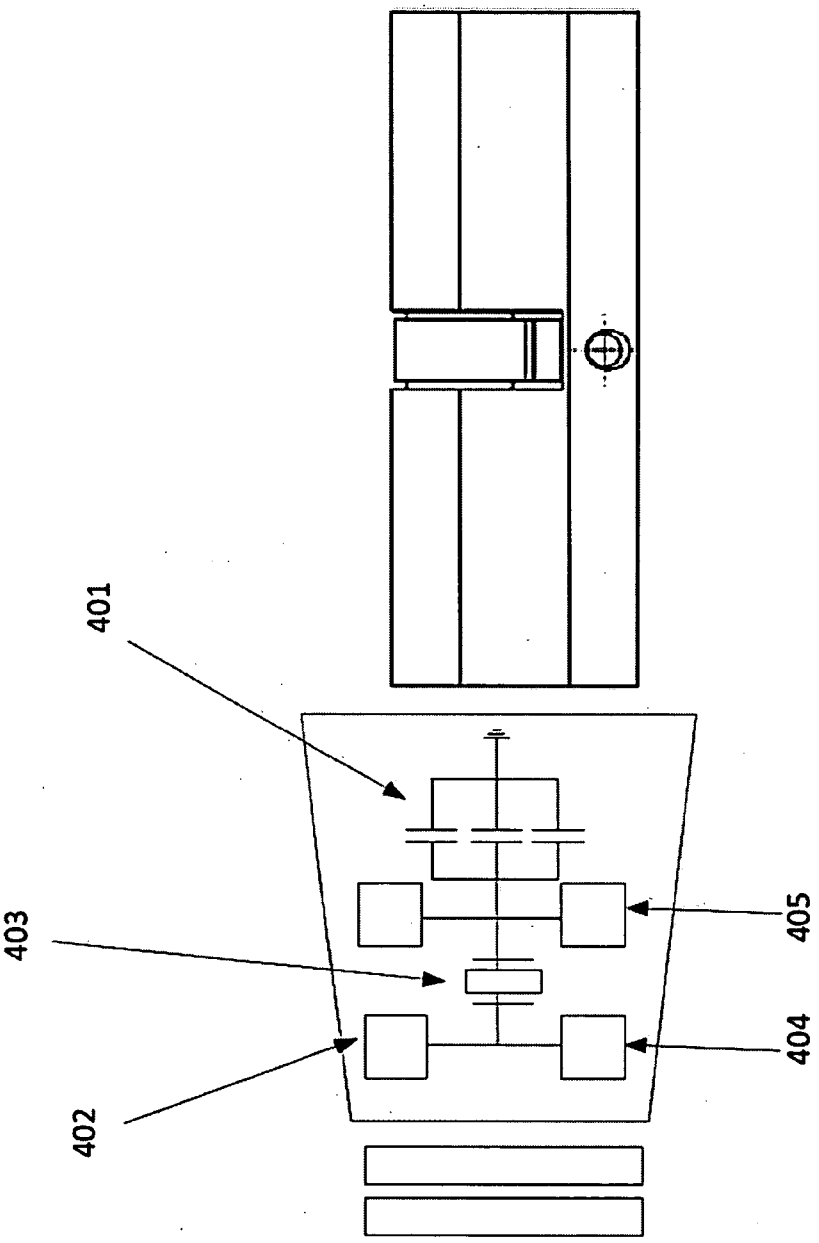


第 3G 圖

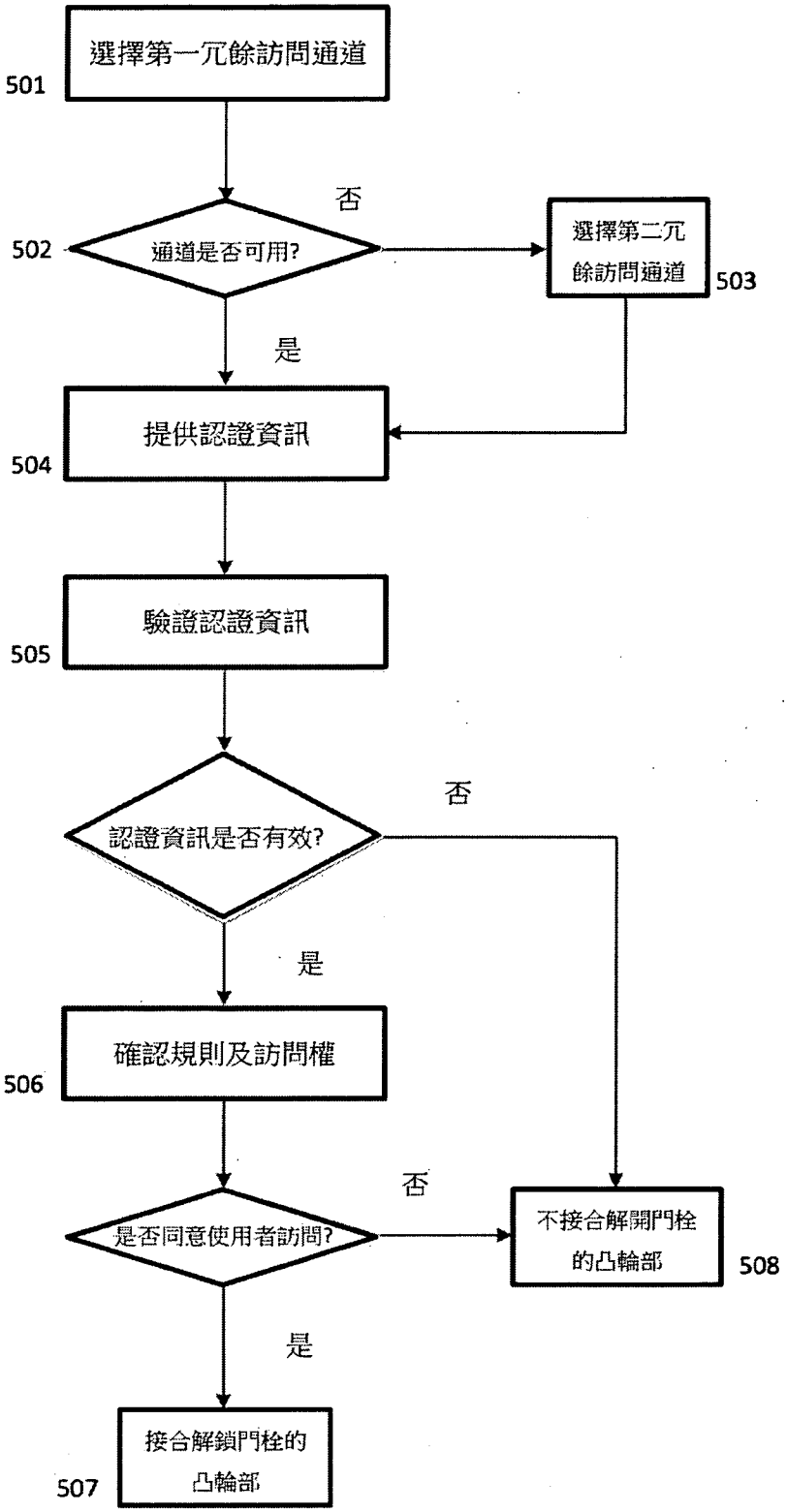


第 3H 圖

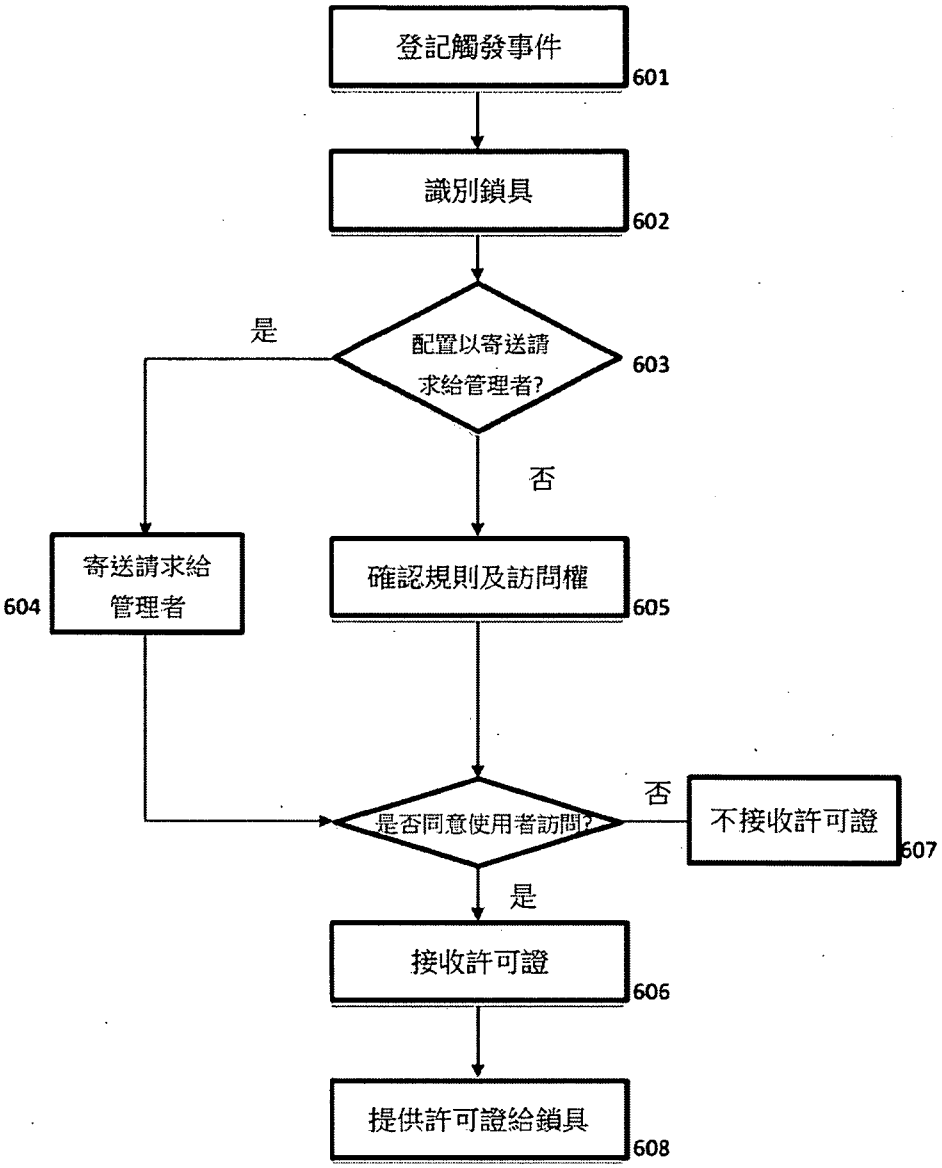




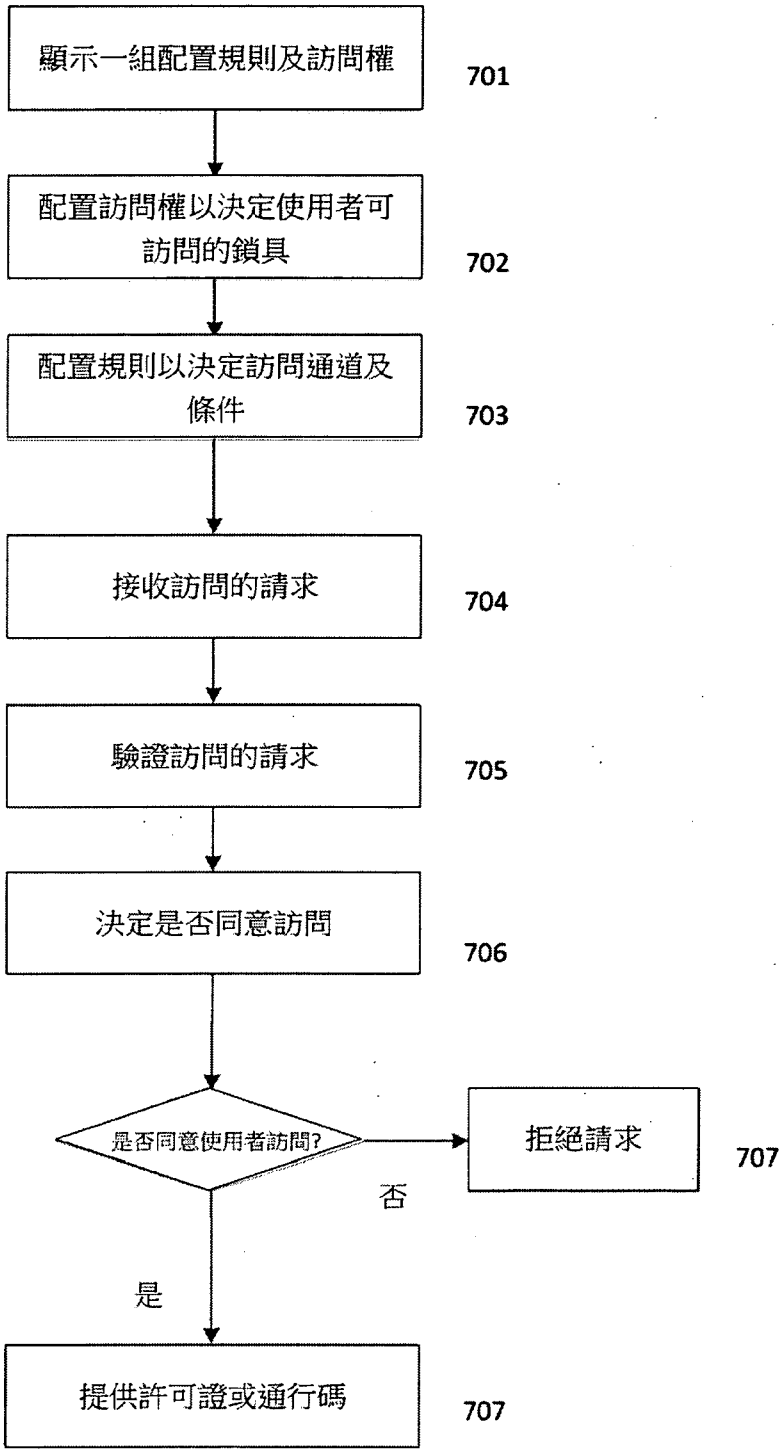
第 4 圖


選擇第一冗餘訪問通道
501
否
502
通道是否可用?
選擇第二冗餘訪問通道
503
是
提供認證資訊
504
驗證認證資訊
505
否
認證資訊是否有效?
是
確認規則及訪問權
506
否
是否同意使用者訪問?
不接合解開門栓的凸輪部
508
是
接合解鎖門栓的凸輪部
507

第 5 圖


登記觸發事件
601
識別鎖具
602
配置以寄送請求給管理者?
603
是
否
寄送請求給管理者
604
確認規則及訪問權
605
是否同意使用者訪問?
否
不接收許可證
607
是
接收許可證
606
提供許可證給鎖具
608

第 6 圖


顯示一組配置規則及訪問權
701
配置訪問權以決定使用者可訪問的鎖具
702
配置規則以決定訪問通道及條件
703
接收訪問的請求
704
驗證訪問的請求
705
決定是否同意訪問
706
是否同意使用者訪問?
拒絕請求
707
否
是
提供許可證或通行碼
707

第 7 圖