I808317

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I808317 B**

(45)公告日： 中華民國 112 (2023) 年 07 月 11 日

(21)申請案號：109111377 (22)申請日： 中華民國 109 (2020) 年 04 月 01 日

(51)Int. Cl.： ***H04L9/30*** ***(2006.01)*** ***H04L9/08*** ***(2006.01)***

(71)申請人：阿證科技股份有限公司 (中華民國) AHP-TECH INC. (TW)

新北市石碇區碇坪路 1 段 50 之 1 號 2 樓

(72)發明人：陳朝煌 CHEN, CHAO-HUANG (TW)

(74)代理人：賴安國；王立成；余宗學

(56)參考文獻：

TW I613899B CN 1957553B

CN 102739395B

審查人員：許人偉

申請專利範圍項數：15 項 圖式數：8 共 59 頁

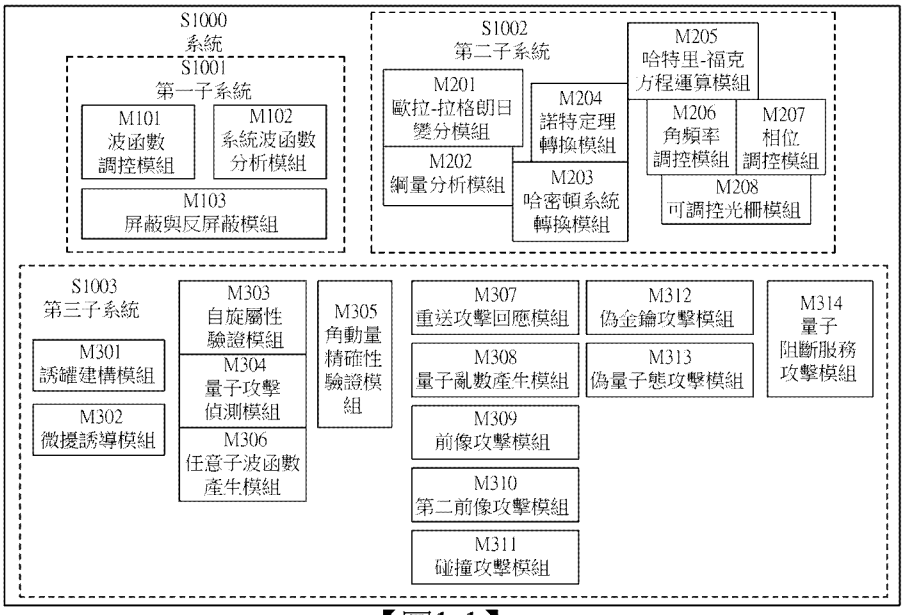
(54)名稱

用於金鑰管理機制的抗量子運算之系統

(57)摘要

一種用於金鑰管理機制的抗量子運算之系統，為一通用性的量子資安解決方案，可用以偵測量子攻擊、迴避量子攻擊，以及反擊量子攻擊等技術手段，可在量子金鑰儲存、量子金鑰消除，以及量子金鑰回收等不同金鑰管理階段，提供一般量子金鑰管理系統完整的對抗架構。在量子金鑰儲存階段，可避免他方量子攻擊對金鑰的篡改、破壞、偵測與封鎖；在量子金鑰消除階段，可避免他方量子攻擊對金鑰糾纏屬性的窺探；在量子金鑰回收階段，可造成他方量子攻擊對金鑰驗證程序的誤判，並消耗攻擊方的運算資源。這是目前多數的 PQC(Post-quantum cryptography)系統所無法提供的防護機制。

指定代表圖：



【圖1-1】

符號簡單說明：

S1000:系統

S1001:第一子系統

S1002:第二子系統

S1003:第三子系統

M101:波函數調控模組

M102:系統波函數分析模組

M103:屏蔽與反屏蔽模組

M201:歐拉-拉格朗日變分模組

M202:綱量分析模組

M203:哈密頓系統轉換模組

M204:諾特定理轉換模組

M205:哈特里-福克方程運算模組

M206:角頻率調控模組

M207:相位調控模組

M208:可調控光柵模組

M301:誘罐建構模組

M302:微擾誘導模組

M303:自旋屬性驗證模組

M304:量子攻擊偵測模組

M305:角動量精確性驗證模組

M306:任意子波函數產生模組

M307:重送攻擊回應模組

M308:量子亂數產生模組

M309:前像攻擊模組

M310:第二前像攻擊模組

M311:碰撞攻擊模組

M312:偽金鑰攻擊模組

M313:偽量子態攻擊模組

M314:量子阻斷服務攻擊模組

公告本 111年7月22日 所提修正

I808317

【發明摘要】

【中文發明名稱】 用於金鑰管理機制的抗量子運算之系統

【中文】

一種用於金鑰管理機制的抗量子運算之系統，為一通用性的量子資安解決方案，可用以偵測量子攻擊、迴避量子攻擊，以及反擊量子攻擊等技術手段，可在量子金鑰儲存、量子金鑰消除，以及量子金鑰回收等不同金鑰管理階段，提供一般量子金鑰管理系統完整的對抗架構。在量子金鑰儲存階段，可避免他方量子攻擊對金鑰的篡改、破壞、偵測與封鎖；在量子金鑰消除階段，可避免他方量子攻擊對金鑰糾纏屬性的窺探；在量子金鑰回收階段，可造成他方量子攻擊對金鑰驗證程序的誤判，並消耗攻擊方的運算資源。這是目前多數的PQC(Post-quantum cryptography)系統所無法提供的防護機制。

【指定代表圖】 圖1-1

【代表圖之符號簡單說明】

S1000 系統

S1001 第一子系統

S1002 第二子系統

S1003 第三子系統

M101 波函數調控模組

M102 系統波函數分析模組

M103 屏蔽與反屏蔽模組

M201 歐拉-拉格朗日變分模組

M202	綱量分析模組
M203	哈密頓系統轉換模組
M204	諾特定理轉換模組
M205	哈特里-福克方程運算模組
M206	角頻率調控模組
M207	相位調控模組
M208	可調控光柵模組
M301	誘罐建構模組
M302	微擾誘導模組
M303	自旋屬性驗證模組
M304	量子攻擊偵測模組
M305	角動量精確性驗證模組
M306	任意子波函數產生模組
M307	重送攻擊回應模組
M308	量子亂數產生模組
M309	前像攻擊模組
M310	第二前像攻擊模組
M311	碰撞攻擊模組
M312	偽金鑰攻擊模組
M313	偽量子態攻擊模組
M314	量子阻斷服務攻擊模組

【發明說明書】

【中文發明名稱】 用於金鑰管理機制的抗量子運算之系統

【技術領域】

【0001】 本發明係關於對抗量子運算攻擊的金鑰管理系統，更特別的是關於一種用於金鑰管理機制的抗量子運算之系統，可用以偵測量子攻擊、迴避量子攻擊，以及反擊量子攻擊等技術手段，可在量子金鑰儲存、量子金鑰消除，以及量子金鑰回收等不同金鑰管理階段，針對量子金鑰藉由光通道進行傳輸時可能遭受到的量子威脅，提供一般量子金鑰管理系統完整的對抗架構。

【先前技術】

【0002】 目前常見的PQC(後量子加密)技術，對於抵抗量子運算的攻擊，大多著重在量子金鑰的產製方法以及量子金鑰的交換過程，然而對於整個完整的金鑰管理階段，仍然缺乏全面性的安全架構；尤其在量子金鑰儲存、量子金鑰消除，以及量子金鑰回收(更新)等過程，特別容易存在量子運算攻擊的漏洞；如果在金鑰管理階段如果缺少抗量子攻擊的安全機制，將使得量子金鑰的產業實用性大打折扣。

【0003】 例如，在量子金鑰儲存階段，來自他方的量子攻擊可能對量子金鑰進行篡改、破壞、偵測與封鎖；在量子金鑰消除階段，來自他方的量子攻擊可能對金鑰糾纏屬性進行窺探；在量子金鑰回收(更新)階段，來自他方的量子攻擊可能對金鑰驗證程序實施中間人攻擊等。

【0004】 由此可知，目前後量子加密之金鑰技術，在金鑰管理階段的配套安全架構仍有待改進。

【發明內容】

【0005】 本發明之一目的在於提出一種能夠對抗量子運算攻擊的用於金鑰管理安全機制的系統，如果能夠在量子金鑰管理的各個階段對抗量子運算的攻擊，才能有效地維護量子金鑰的實用性。此技術可實現於具合理成本的電子裝置或系統，且可用於保護多數的量子金鑰管理系統。同時有效避免先前技術在現行PQC方案的實作漏洞、以及解決一般安全機制對於量子運算攻擊缺乏反擊能力等問題。

【0006】 為達成上述目的，本發明提出一種用於金鑰管理機制的抗量子運算之裝置或系統的實施例，可包含有以下一個或多個子系統：一第一子系統，可在量子金鑰儲存階段，避免來自他方的量子攻擊可能對量子金鑰進行篡改、破壞、偵測與封鎖；一第二子系統，可在量子金鑰消除階段，避免來自他方的量子攻擊可能對金鑰糾纏屬性進行窺探；以及一第三子系統，可在量子金鑰回收階段，避免來自他方的量子攻擊可能對金鑰驗證程序實施中間人攻擊等。而上述之『量子金鑰回收階段』，包括相關習知領域所稱之金鑰回收、金鑰更新或金鑰輪替等相關程序或管理階段。

【0007】 其中，該第一子系統，為避免系統所儲存的量子金鑰受到他方量子運算的竄改或破壞，需包含以下模組：一『波函數調控模組』，可運用薛丁格方程式藉由動量調整而改變波函數；一『系統波函數分析模組』，可經由絕熱近似的計算機制，估計出他方量子運算所使用的波函數；以及一『屏蔽與反屏蔽模組』，可避免儲存中的量子金鑰受到他方量子運算的偵測或封鎖。

【0008】 在一實施例中，上述之系統波函數分析模組為了根據對量子通訊環境的量測結果，有效率地推估出攻擊方的波函數，更包含有以下子單元：一『二次量子化計算子單元』，一『GW近似法計算子單元』，一『WKB近似法計算子單元』，一『變分近似法計算子單元』，一『斯萊特行列式計算子單元』，一『包利矩陣轉換子單元』，一『玻恩定則運算子單元』，一『法蘭克-康登原理分析子單元』，以及一『絕熱近似運算子單元』。

【0009】 上述該二次量子化計算子單元，可針對無法判斷量子攻擊屬性來自於玻色子還是費米子的狀況，使用創生與湮滅算符(creation and annihilation operators)進行諧振子分析，可用於量測計算經過二次量子化所發動的諧振子攻擊；該GW近似法計算子單元，可針對因利用遮蔽效應而無法進行泛函分析的量子攻擊，使用GW近似法做量測計算，亦可針對激發態的量子攻擊採用GW近似法搭配微擾項進行量測；該WKB近似法計算子單元，則可特別針對波函數變化緩慢的量子攻擊，以WKB近似法進行推估量測；以及該變分近似法計算子單元，則是特別針對波函數變異快速的量子攻擊，透過泛函分析的變分法進行推估量測。以上四個子單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，但在一些實施例中，此組合可整合為一量子系統量測單元，可涵蓋對多種可實施的量子攻擊之波函數進行有效量測，可實做為一通用型的量子攻擊偵測元件。

【0010】 接著，上述該斯萊特行列式計算子單元，可將來自上述整合之量子系統量測單元多個波函數量測結果轉換成斯萊特行列式(Slater determinant)的形式；而後，該包利矩陣轉換子單元，再將斯萊特行列式轉換成多個包利矩陣(Pauli matrices)以表達多個觀測值；該玻恩定則運算子單元，可利用玻恩定則

(Born rule)推算各觀測值的對應躍遷機率；再經由該法蘭克-康登原理分析子單元，運用法蘭克-康登原理(Franck-Condon principle)的量子力學公式，可將推算出的量子諧振子函數與躍遷機率進行分析，導出量子波函數與核波函數的近似解；最後再透過該絕熱近似運算子單元，利用量子波函數與核波函數的近似解以絕熱近似運算可得一整體波函數之近似解，以做為所測定之量子系統波函數。以上五個子單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，但在一些實施例中，此組合可整合為一系統波函數分析單元，可達成先前技術未提供之快速測定量子系統波函數之功效。

【0011】 在同一實施例中，為將多個波函數量測所導出的結果，表示為一初始平衡態以便進行絕熱近似運算，上述之系統波函數分析模組中的絕熱近似運算子單元需進一步包含以下子模組：一射影計算子模組；一福克空間轉換子模組；一希爾伯特變換子模組；一二次量子化子模組；一傅立葉轉換子模組；一泛函分析子模組；一歸一化運算子模組；一總均計算子模組；以及一薛丁格方程轉換子模組。其中，『射影計算』子模組，可根據量子波函數與核波函數的近似解，利用射影算子(projection operator)，推估所量測的量子系統其量子比特(Qubit)的線性組合；再透過『福克空間轉換』子模組，將量子比特的線性組合以福克空間(Fock Space)的奇異積分算子(singular integral operator)表示為一量子系統態；接著使用『希爾伯特變換』子模組，將福克空間的量子系統態轉換至多維度的希爾伯特空間(Hilbert space)；而後透過『二次量子化』子模組，利用創生與湮滅算符對希爾伯特空間的量子系統態進行二次量子化，其結果可用於描述量子系統的哈密頓量；接著經由『傅立葉轉換』子模組，將量子系統的哈密頓量進行傅立葉轉換，以消除位置與動量等物理量的不確定性；然後使用『泛函分析』子模組，

以變分法對已確定的轉換後系統物理量做分析，以獲得可代表波函數特性的機率分布；再以『歸一化運算』子模組，將該機率分布進行歸一化程序；並以『總均計算』子模組，根據已歸一化的機率分布估計總體均值；最後再利用『薛丁格方程轉換』子模組，根據所估計的總體均值、機率分布，以及已確定的物理量，將此量子系統態以一時間相關的薛丁格方程式表示，以做為絕熱近似運算所需的初始平衡態。以上九個子模組可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可整合於一絕熱近似運算子單元，可達成先前技術未提供之以模組化近似運算，進行高效推估量子系統波函數之功能。

【0012】 在同一實施例中，上述之第一子系統會根據系統波函數分析模組的計算結果，判斷量子通訊環境是否存在異常的量子系統波函數，以決定是否需啟動屏蔽或反屏蔽機制，並配合波函數的調控，以避免系統所儲存的量子金鑰受到他方量子運算的竄改或破壞。

【0013】 為此，在同一實施例中，上述之『屏蔽與反屏蔽模組』需包含有一角動量耦合單元；一自旋軌道耦合單元；一重原子效應產生單元；一耦合常數導出單元；以及一動能強度對應單元。其中，『角動量耦合單元』，可用於根據系統波函數分析模組所測得的異常波函數，耦合出對應的自旋角動量；『自旋軌道耦合單元』，採用j-j耦合(J-J Coupling)程序，可進行軌道與自旋角動量的耦合；『重原子效應產生單元』，則是經由增強自旋軌道的耦合效應，可進一步激發躍遷效應；該子系統可藉此以上三個單元的組合，實施為一反屏蔽機制，以避免攻擊方利用屏蔽攻擊而封鎖一般量子金鑰的遠端存取。

【0014】 此外，上述屏蔽與反屏蔽模組之『耦合常數導出單元』，藉由計算躍遷效應之發生機率，可進一步推導出耦合常數；其『動能強度對應單元』，

則根據耦合常數與動能的關係，建立耦合常數與動能強度的對應資料，可進一步提供該子系統透過波函數調控模組進行波函數調控時，所需的動量參數；該子系統可藉此以上兩個單元的組合，實施為一屏蔽機制，經由改變量子通道的系統波函數，以避免攻擊方利用量子通訊通道，偵測儲存中的量子金鑰組態之波函數。以上五個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可整合為一屏蔽與反屏蔽模組，可達成先前技術未提供之避免量子金鑰的存取被封鎖以及避免量子金鑰組態之波函數被偵測之功能。

【0015】 在另一實施例中，關於依據本發明之第二子系統，為推導出可改變光通訊通道之折射率的動能項，至少需包括以下模組：一『歐拉-拉格朗日變分模組』；一『綱量分析模組』；以及一『哈密頓系統轉換模組』。其中，歐拉-拉格朗日變分模組，可進行時間與光路徑的變分運算，並以歐拉-拉格朗日方程(Euler-Lagrange equation)的表述推導出最小作用量的穩定值；綱量分析模組，可接著將該最小作用量的穩定值透過綱量，轉換為一與動量相關之表述；哈密頓系統轉換模組，可根據該動量相關之表述轉換為辛空間之廣義動量，並利用其二次型導出動能項。

【0016】 為使該子系統可進一步利用上述哈密頓系統轉換模組所導出的動能項，以實現其調控折射率之能力，該第二子系統應再包含以下模組：一『諾特定理轉換模組』；一『哈特里-福克方程運算模組』；一『角頻率調控模組』；一『相位調控模組』；以及一『可調控光柵模組』。其中，諾特定理轉換模組，可根據上述哈密頓系統轉換模組所導出的動能項，以諾特定理(Noether's theorem)轉換為具備一般全局對稱性之角動量守恆量；哈特里-福克方程運算模組，可利用哈特里-福克方程式(Hartree-Fock equation)計算打破該角動量守恆量所需的最

低動能；接著，該子系統可根據最低動能的需求，使用角頻率調控模組與相位調控模組，進行角頻率與相位的調控；最後，再透過可調控光柵模組，可將完成角頻率與相位調控程序的光波導入以電光晶體實作的光柵元件，因角動量的守恆量被打破，使得折射率產生所需的變動。

【0017】 以上八個模組可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可整合於一第二子系統，可於量子金鑰消除的過程中，利用對現有光通訊環境之路徑折射率的暫時改變，使得攻擊方無法經由量子通道觀察量子金鑰消除過程中相關系統物理量的變化，再利用量子運算分析出量子金鑰在製備時所採用的自旋屬性。此一量子金鑰消除過程中的保護機制，為先前技術所無法達到之功效。

【0018】 在另一實施例中，為對抗針對量子金鑰回收過程所發動的量子運算攻擊(本發明所稱金鑰回收，包含相關領域所指的金鑰回收、更新或輪替等相關程序)，可實作一第三子系統，至少包含以下模組：一『誘罐建構模組』，可建構特定誘罐(Honeypot)，用於觀察在量子金鑰回收過程中，來自他方量子運算攻擊的可能行為；以及一『微擾誘導模組』，可根據誘罐建構模組的運算結果，進行微擾誘導(Perturbation Induction)程序，以轉移量子金鑰回收過程中，來自他方量子運算的攻擊。

【0019】 其中，該誘罐建構模組包含有以下單元：一『多微波產生單元』，可利用多組不同共振頻率的微波產生器，與光量子作用出不同的躍遷效應；一『可調控位能井單元』，實作一位能井(potential well)，利用散射與微擾程序，產生能級偏移，以便控制躍遷機率的範圍；一『角頻率配製單元』，將費米黃金定律(Fermi's golden rule)運用於離散能階躍遷，根據所需的角頻率導出態密度，

並搭配散射理論之玻恩近似法(Born approximation)推導出對應的散射截面與入射角度，可用於配製做為自旋屬性的角頻率；一『激發態機率分析單元』，可根據高能階至低能階所量測到的光電效應，估算激發態機率，分析是否需要對位能井進行調控；以及一『單頻諧波分析單元』，將所配製之角頻率以單頻諧波表達，再與量測到的躍遷機率分佈做比對分析，以驗證所配製的角頻率是否適用。以上五個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可彈性且及時調整出所需的躍遷特徵與角頻率特徵，以便觀察各種不同的量子攻擊行為，此為先前技術所無法達到之功效。

【0020】 另外，在同一實施例中，上述微擾誘導模組，至少包含以下單元：一『布洛赫球監控單元』，實作一具布洛赫球(Bloch sphere)座標體系之監視裝置，用於觀察、標定並分析來自他方的量子運算行為；一『角動量合成單元』，根據布洛赫球的監控分析結果，可透過誘罐建構模組使用不同的角頻率合成所需的角動量；以及一『諧波產生單元』，可產生角動量所對應的諧波，以微擾程序誘導人造原子產生偏移，可轉移來自他方的量子攻擊。以上三個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可彈性且及時轉移攻擊方的量子偵測行為，以避免攻擊方測得真正的量子金鑰相關資訊。此一可實施於量子金鑰的發送端與接收端或於量子通道上的第三端的誘導移轉保護機制，為先前技術所無法達到之功效。

【0021】 在另一實施例中，為強化對量子運算攻擊的偵測與反擊能力，上述之第三子系統，可再更進一步包含以下模組：一『自旋屬性驗證模組』，可導出量子自旋屬性之拓樸性質、動量性質，以及偏振性質，以分析量子是否具有特定的自旋屬性；一『量子攻擊偵測模組』，可分析變形的量子運算攻擊，並根據

共同基底與變化區間，協同自旋屬性驗證模組，可進一步鎖定惡意的量子攻擊；一『任意子波函數產生模組』，可利用任意子(anyon)的二維模型，調控角動量，以改變自旋角度循環生成多種波函數，可混淆來自他方的量子運算；以及一『角動量精確性驗證模組』，運用微擾理論，可提供該子系統各單元或各模組驗證計算其角動量的精確性是否適用。

【0022】 其中，上述之自旋屬性驗證模組，包含有以下單元：一『投影量子數分析單元』，可對波函數異常的通訊環境進行分析，得到多重自旋態的自旋投影量子數；一『包利向量分析單元』，將多重態的自旋投影量子數透過包利向量(Pauli vector)與歐拉公式，可得一複平面座標做為量子自旋屬性之拓樸不變量；一『簡諧振子分析單元』，可分析量子系統之簡諧振子的角頻率線性組合與相位線性組合，以做為量子自旋屬性的動量特徵；以及一『光路徑分析單元』，可分析通訊環境之光路徑的折射率以及散射角度的組合，以做為量子自旋屬性的偏振特徵。以上四個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之自旋屬性驗證模組，可整合得到量子自旋屬性之拓樸性質、動量性質，以及偏振性質，可鎖定特定自旋屬性的組合做為量子系統特徵，以驗證量子通訊環境中是否具備應該警示的量子系統特徵，此為先前技術所無法達到之功效。

【0023】 在同一實施例中，上述之量子攻擊偵測模組，則包含有以下單元：一『角動量相容觀察單元』，利用哈密頓算符與角動量算符的對易關係，可量測出兩者共同本徵值的變化區間，並導出角動量與量子系統共同的本徵態；一『不相容可觀察量驗證單元』，可對一量子測量其哈密頓量，再對另一量子測量其角動量，若此兩種量子可觀察量之不確定性乘積無法證明其互為不相容可觀察量，

則可驗證此二量子態具有共同基底；以及一『異常變動偵測單元』，可根據偵測通訊環境之量子系統的異常變化，回饋該第三子系統，以協同角動量相容觀察單元與不相容可觀察量驗證單元確認是否存在可疑的變形量子攻擊。以上三個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之量子攻擊偵測模組，可藉由對量子系統物理量與角動量的觀察與分析，可測定是否存在與特定量子態具有共同基底的變形量子攻擊，可實施為量子系統的資安黑名單機制，此為先前技術所無法達到之功效。

【0024】 此外，在同一實施例中，為完備上述量子攻擊偵測模組之異常變動偵測單元，該單元進一步包含有以下子單元：一『異常退相干偵測子單元』，可根據對量子通訊環境所偵測的退相干速率，判斷是否回饋該第三子系統一異常訊號；一『波函數坍縮偵測子單元』，可對量子通訊環境進行波函數監控，若偵測到可能因中間人量子攻擊而導致的波函數坍縮現象，則回饋該第三子系統一異常訊號；一『異常躍遷偵測子單元』，可根據對量子通訊環境所偵測的躍遷機率，判斷是否回饋該第三子系統一異常訊號；一『異常變數偵測子單元』，導入EPR悖論(Einstein-Podolsky-Rosen paradox)分析程序，若偵測到量子通訊環境的一量子物理行為同時符合定域實在論與不確定原理，表示可能存在異常環境變數，則回饋該第三子系統一異常訊號；以及一『異常熵變動偵測子單元』，可根據偵測通訊環境之量子系統的熵(entropy)變化程度，判斷是否回饋該第三子系統一異常訊號。以上五個子單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之異常變動偵測單元，可藉由監控量子通訊環境的系統變化，有效示警通訊環境中異常的量子行為，在一些實施例中，亦

可進一步被第一或第二子系統使用，以提供量子金鑰管理系統不同階段的示警，此為先前技術所無法達到之功效。

【0025】 另外，在同一實施例中，有關上述第三子系統之角動量精確性驗證模組，則進一步包含有以下單元：一『零微擾波函數計算單元』，利用零微擾哈密頓量、總角動量平方、軌道角動量平方以及自旋角動量平方等四個算符的共同本徵函數做為零微擾波函數，可計算出一階能量位移；以及一『能量位移驗證單元』，利用計算出的一階能量位移與量測到的能級偏移作比對，以確認估算出的角動量其精確性是否適用。以上兩個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之角動量精確性驗證模組，藉由搭配微擾理論的實作，可提升角動量估算的精度，除可確保角動量可做為依據本發明實施例之系統重要的內稟屬性(intrinsic property)外；同時可提升該第三子系統之微擾誘導模組，其角動量合成的準確性；此外亦可支援依據本發明實施例之第二子系統在實施諾特定理轉換時，所導出的角動量守恆量之正確性；除了正確性的考量外，本驗證模組亦可協助依據本發明實施例之第三子系統以微擾誘導模組實施微擾誘導程序時，進行一級或二級能量與波函數的微擾修正，以確保微擾誘導程序的能級偏移符合需求；最重要的是，若角動量計算的誤差過大，亦可能影響上述自旋屬性驗證模組的判斷結果，故此模組對維護整個系統的警示機制亦有關鍵作用；以上皆為先前技術所未實施之功效。

【0026】 在一些實施例中，為進一步降低上述角動量精確性驗證模組之驗證誤差，該模組之能量位移驗證單元可再包含以下子單元：一『簡併能階分析子單元』，利用對自旋量子數的狀態分析，可判斷目前的能量位移是否為一簡併態；一『質量干擾分析子單元』，利用分析質量解析度，可判斷目前的能量位移是否

存在質量干擾；以及一『蘭姆位移測定子單元』，若能量位移量測的結果可確認為簡併態且存在質量干擾，則可採用蘭姆位移(Lamb shift)之計算進行能級偏移分析。以上三個子單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之能量位移驗證單元，可在能量位移受到簡併態與質量干擾的影響下，仍可維護角動量計算的精確性，此為先前技術所無法達到之功效。

【0027】 在另外一些實施例中，為加強本發明實施例對相關量子運算攻擊的反制能力，其第三子系統可再進一步包含以下模組：一『重送攻擊回應模組』，用於回應攻擊方所發動的重送攻擊(replay attack)；一『量子亂數產生模組』，用於產生一偽造的雜湊值(hash value)或訊息摘要(digest)；一『前像攻擊模組』，採用偽造的雜湊函式(hash function))搭配真實的訊息摘要，用以對攻擊方發動前像攻擊(preimage attack)；一『第二前像攻擊模組』，隱藏真實的雜湊函式，並改變真實訊息摘要的長度，用以對攻擊方發動第二前像攻擊(second-preimage attack)；以及一『碰撞攻擊模組』，以真實雜湊函式的反函式做為雜湊函式，以真實訊息摘要的反元素作為訊息摘要，用以對攻擊方發動多碰撞攻擊(multi-collision attack)。以上五個模組可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然而對於在量子金鑰回收、消除或儲存過程中試圖攔截相關交換訊息的攻擊方，此組合可對其實施基本且有效的反制機制，以避免攻擊方蒐集足夠多的交握訊息而進行破密分析，在一些實施例中，亦可進一步被第一或第二子系統所使用，以提供該量子金鑰管理系統在不同階段被攻擊時的反制機制，此為先前技術所無法達到之功效。

【0028】 最後，在上述實施例中，為再增加本發明實施例對持續性的量子運算攻擊的進階反制能力，其量子金鑰回收子系統可再進一步包含以下模組：一『偽金鑰攻擊模組』，用於對攻擊方發送假造的公開金鑰；一『偽量子態攻擊模組』，使用不正確的自旋屬性組合，產製大量偽造的量子態；以及一『量子阻斷服務攻擊模組』，以阻斷服務(DoS)的攻擊型態，對攻擊方發送大量的退相干組態。以上三個模組可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然而對於在量子金鑰回收、消除或儲存過程中持續性蒐集相關交換訊息的攻擊方，此組合可對其實施進階反制機制，可迅速且有效地消耗攻擊方的量子運算資源，進而癱瘓其在成本考量下有限的量子算力，在一些實施例中，亦可進一步被第一或第二子系統所使用，以提供該量子金鑰管理系統在不同階段被攻擊時的進階反制機制，此為先前技術所無法達到之功效。

【0029】 藉此，上述本發明的多個實施例可實現對抗量子運算攻擊的用於金鑰管理機制的系統，可在量子金鑰儲存、量子金鑰消除，以及量子金鑰回收等不同金鑰管理階段，提供一般量子金鑰管理系統完整的對抗架構。此技術可實現為高強度的抗量子運算之金鑰管理裝置或系統，且可實現於欲進行通訊的發送端與接收端。在一些實施例中，此技術可視系統的資安需求，除了可偵測量子攻擊與迴避量子攻擊之外，還能夠進一步選擇是否實施基本或進階的攻擊反制模組。此外，此系統之相關技術手段皆能透過具合理成本之裝置實現，有效克服現行多數PQC方案須透過高昂成本之設備運作的瓶頸，同時也提供了多數先前技術在現行PQC方案所無法支援量子金鑰管理系統的資安機制。

【圖式簡單說明】

【0030】

圖1-1係本發明之系統的實施例的代表圖。

圖1-2係本發明之用於金鑰管理機制的抗量子運算之系統的實施例的系統架構方塊圖。

圖2係圖1-2之用於金鑰管理機制的抗量子運算之系統的使用情景的實施例的示意圖。

圖3-1係本發明之一實施例的量子金鑰儲存子系統的系統架構方塊圖。

圖3-2係本發明的量子金鑰儲存子系統之一實施例的實施流程示意圖。

圖4係圖3-1中系統波函數分析模組之一實施例的架構方塊圖。

圖5係圖4中絕熱近似運算子單元之一實施例的架構方塊圖。

圖6係本發明之一實施例的量子金鑰回收子系統的系統架構方塊圖。

圖7-1係量子攻擊偵測模組之一實施例之流程示意圖。

圖7-2係圖6中量子攻擊偵測模組與角動量精確性驗證模組之一實施例的架構方塊圖。

圖8係圖7-2中角動量精確性驗證模組與本發明實施例之其他單元之支援關係圖。

【實施方式】

【0031】 為充分瞭解本發明之目的、特徵及功效，茲藉由下述具體之實施例，並配合所附之圖式，對本發明做詳細說明，說明如後：

【0032】 以下提供本發明之系統做為一種抗量子運算之量子金鑰管理系統（或可實現為裝置）的多個實施例，能夠在量子金鑰管理的各個階段對抗量子

運算的攻擊。在一此實施例中，此系統可在量子金鑰儲存、量子金鑰消除，以及量子金鑰回收等不同金鑰管理階段，提供一般量子金鑰管理系統完整的對抗架構。在一些實施例中，此技術可分別實現為高強度的抗量子運算之金鑰管理之裝置或系統，例如實現於欲進行通訊的發送端(金鑰管理單位)或接收端(遠端使用者)的系統（或裝置）。如系統代表圖1-1所示，本發明實施例之系統可包含有一第一子系統S1001，一第二子系統S1002，以及一第三子系統S1003。在多數實施例中，該第一子系統可被實施為一量子金鑰儲存子系統，該第二子系統可被實施為一量子金鑰消除子系統，而該第三子系統可被實施為一量子金鑰回收子系統。

【0033】 舉例而言，如圖1-2所示，用於金鑰管理機制的抗量子運算之系統可包含有以下一個或多個子系統：一『量子金鑰儲存』子系統S1001A，可在量子金鑰儲存階段，避免來自他方的量子攻擊可能對量子金鑰進行篡改、破壞、偵測與封鎖；一『量子金鑰消除』子系統S1002A，可在量子金鑰消除階段，避免來自他方的量子攻擊可能對金鑰糾纏屬性進行窺探；以及一『量子金鑰回收』子系統S1003A，可在量子金鑰回收階段，避免來自他方的量子攻擊可能對金鑰驗證程序或交握訊息實施中間人攻擊等。本發明之相關實施例所稱之『量子金鑰回收階段』，包括相關習知領域所稱之金鑰回收、金鑰更新或金鑰輪替等相關程序或管理階段。

【0034】 關於依據本發明之實施例的用於金鑰管理機制的抗量子運算之系統(以下稱系統S1000A)，請參閱圖1-2所示，系統S1000A其可實施的子系統有：『量子金鑰儲存』子系統S1001A；『量子金鑰消除』子系統S1002A；以及『量子金鑰回收』子系統S1003A。請再參考圖2，其為圖1-2之用於金鑰管理機制的抗量子運算之系統的使用情景的實施例示意圖。如圖2所示，遠端通訊裝置10、金

鑰管理裝置20以一通訊連結LK進行通訊，本發明實施例之通訊連結LK主要是基於量子通訊的光傳輸通道；遠端通訊裝置10、金鑰管理裝置20分別裝設或實現了如圖1-2所示意的用於金鑰管理機制的抗量子運算之系統S1000並連接至遠端通訊裝置10、金鑰管理裝置20中各自的通訊模組100、200，其中通訊模組可透過通訊連結LK進行訊號發送或接收金鑰。裝置10、20可進行各種如習知的金鑰管理程序(例如量子金鑰儲存、量子金鑰消除以及量子金鑰回收等)，其中通訊連結LK實現為量子通訊通道。裝置10、20因為分別裝設或實現了如圖1-2所示意的用於金鑰管理機制的抗量子運算之系統S1000並使用於金鑰管理程序中，故可於金鑰管理的不同階段產生可對抗量子運算攻擊之效果。換言之，本系統於量子金鑰的儲存階段可協調該量子金鑰儲存子系統(第一子系統)針對來自他方的量子攻擊可能對量子金鑰進行篡改、破壞、偵測與封鎖提供安全機制；並進一步於量子金鑰的消除階段協調該量子金鑰消除子系統(第二子系統) 防制來自他方的量子攻擊對金鑰糾纏屬性進行窺探；並且於量子金鑰的回收階段協調該量子金鑰回收子系統(第三子系統) 避免來自他方的量子攻擊可能對金鑰驗證程序或交握訊息實施中間人攻擊等。

【0035】 在一實施例中，為了在金鑰管理的量子金鑰儲存階段具備對抗量子運算攻擊的安全機制，避免系統所儲存的量子金鑰受到他方量子運算的竄改或破壞，本發明實施例提供一如圖3-1所示之量子金鑰儲存子系統S1001A包含以下模組：一『波函數調控模組』M101；一『系統波函數分析模組』M102；以及一『屏蔽與反屏蔽模組』M103。其中，1)首先該波函數調控模組M101，利用薛丁格方程式藉由動量調整而改變波函數；2)其次該系統波函數分析模組M102，經由絕熱近似的計算機制，估計出他方量子運算所使用的波函數；再協同3)該屏

蔽與反屏蔽模組M103提供屏蔽與反屏蔽機制以避免儲存中的量子金鑰受到他方量子運算的偵測或封鎖。藉由以上模組M101~M103之組合以支持該量子金鑰儲存子系統S1001A在金鑰管理的量子金鑰儲存階段提供對抗量子運算攻擊的安全機制。

【0036】 參考圖4，在同一實施例中，上述之系統波函數分析模組M102為了根據對量子通訊環境的量測結果，有效率地推估出攻擊方的波函數，可實作以下子單元：一『二次量子化計算子單元』U10101，一『GW近似法計算子單元』U10102，一『WKB近似法計算子單元』U10103，一『變分近似法計算子單元』U10104，一『斯萊特行列式計算子單元』U10201，一『包利矩陣轉換子單元』U10202，一『玻恩定則運算子單元』U10203，一『法蘭克-康登原理分析子單元』U10204，以及一『絕熱近似運算子單元』U10205。

【0037】 其中，上述之系統波函數分析模組M102為涵蓋對多種可實施的量子攻擊之波函數進行有效量測，可執行以下操作：1)針對無法判斷量子攻擊屬性來自於玻色子還是費米子的狀況，可呼叫該二次量子化計算子單元U10101使用創生與湮滅算符(creation and annihilation operators)進行諧振子分析，以便量測計算經過二次量子化所發動的諧振子攻擊；2)針對因利用遮蔽效應而無法進行泛函分析的量子攻擊，可呼叫該GW近似法計算子單元U10102使用GW近似法做量測計算；3)亦可針對激發態的量子攻擊呼叫該GW近似法計算子單元U10102採用GW近似法搭配微擾項進行量測；4)對於對波函數變化緩慢的量子攻擊，則呼叫該WKB近似法計算子單元U10103以WKB近似法進行推估量測；以及5)特別針對波函數變異快速的量子攻擊，則呼叫該變分近似法計算子單元U10104透過泛函分析的變分法進行推估量測。以上U10101~U10104四個子單元可基於相關之習

知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，但在一些實施例中，此組合可整合為一如圖4所示之量子系統量測單元U101，可涵蓋對多種可實施的量子攻擊之波函數進行有效量測，可實做為一通用型的量子攻擊偵測元件。

【0038】 參考圖4，在上述實施例中，該系統波函數分析模組M102所內建的斯萊特行列式計算子單元U10201，可將來自上述整合之量子系統量測單元U101的多個波函數量測結果轉換成斯萊特行列式(Slater determinant)的形式；而後，該包利矩陣轉換子單元U10202，再將斯萊特行列式轉換成多個包利矩陣(Pauli matrices)以表達多個觀測值；該玻恩定則運算子單元U10203，可利用玻恩定則(Born rule)根據U10202的轉換結果，推算各觀測值的對應躍遷機率；再經由該法蘭克-康登原理分析子單元U10204，運用法蘭克-康登原理(Franck-Condon principle)的量子力學公式，可將推算出的量子諧振子函數與U10203所導出的躍遷機率進行分析，估算出量子波函數與核波函數的近似解；最後再透過該絕熱近似運算子單元U10205，利用U10204所估算的量子波函數與核波函數的近似解進行絕熱近似運算可得一整體波函數之近似解，以做為所測定之量子系統波函數。以上U10201~U10205五個子單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，但在一些實施例中，此組合可整合為一系統波函數分析單元U102，藉由量子系統量測單元U101與系統波函數分析單元U102的協同運作，使得系統波函數分析模組M102可達成先前技術未提供之快速測定量子系統波函數之功效。

【0039】 在同一實施例中，參考圖5，為將多個波函數量測從U101到U10201，U10202，U10203，乃至U10204所導出的結果，表示為一初始平衡態以便進行絕熱近似運算，上述之系統波函數分析模組M102中的絕熱近似運算子單

元U10205需進一步實作以下子模組：一射影計算子模組M10201；一福克空間轉換子模組M10202；一希爾伯特變換子模組M10203；一二次量子化子模組M10204；一傅立葉轉換子模組M10205；一泛函分析子模組M10206；一歸一化運算子模組M10207；一總均計算子模組M10208；以及一薛丁格方程轉換子模組M10209。首先，『射影計算』子模組M10201，可根據來自上述法蘭克-康登原理分析子單元U10204的量子波函數與核波函數的近似解，利用射影算子(projection operator)，推估所量測的量子系統其量子比特(Qubit)的線性組合；再透過『福克空間轉換』子模組M10202，將該量子比特的線性組合以福克空間(Fock Space)的奇異積分算子(singular integral operator)表示為一第一量子系統態；接著使用『希爾伯特變換』子模組M10203，將福克空間的該第一量子系統態轉換至多維度的希爾伯特空間(Hilbert space)而得一第二量子系統態；而後透過『二次量子化』子模組M10204，利用創生與湮滅算符對希爾伯特空間的該第二量子系統態進行二次量子化，其結果可用於描述量子系統的整體物理量而得一哈密頓量；接著經由『傅立葉轉換』子模組M10205，將量子系統的該哈密頓量進行傅立葉轉換，以消除位置與動量等物理量的不確定性，以得到一轉換後的系統物理量；然後使用『泛函分析』子模組M10206，以變分法對已確定的轉換後系統物理量做分析，以獲得可代表波函數特性的機率分布；再以『歸一化運算』子模組M10207，將該機率分布進行歸一化程序，得到一已歸一化的機率分布；並以『總均計算』子模組M10208，根據已歸一化的機率分布估計總體均值；最後再利用『薛丁格方程轉換』子模組M10209，根據所估計的該總體均值、機率分布，以及已確定的物理量，將此量子系統態以一時間相關的薛丁格方程式表示，以做為絕熱近似運算所需的初始平衡態。以上M10201~M10209九個子模組可基於相關之習知技術

而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可整合於一絕熱近似運算子單元U10205，可達成先前技術未提供之以模組化近似運算，進行高效推估量子系統波函數之功能。

【0040】 在同一實施例中，參考圖3-2所示流程，上述之量子金鑰儲存子系統S1001A會根據系統波函數分析模組M102的計算結果，判斷量子通訊環境是否存在異常的量子系統波函數，以決定是否呼叫屏蔽與反屏蔽模組M103啟動屏蔽或反屏蔽機制，並透過波函數調控模組M101進行波函數的調控，以避免系統所儲存的量子金鑰受到他方量子運算的竄改或破壞。

【0041】 為此，如圖3-1所示，在同一實施例中，上述之『屏蔽與反屏蔽模組』M103需包含有一角動量耦合單元U103；一自旋軌道耦合單元U104；一重原子效應產生單元U105；一耦合常數導出單元U106；以及一動能強度對應單元U107。參考圖3-2的流程，其中，『角動量耦合單元』U103，可用於根據系統波函數分析模組M102所測得的異常波函數，耦合出一對應的第一自旋角動量；『自旋軌道耦合單元』U104，採用j-j耦合(J-J Coupling)程序，可進行具異常波函數之攻擊方的量子軌道與該第一自旋角動量的耦合；『重原子效應產生單元』U105，則是經由增強U104自旋軌道的耦合效應，可進一步改變攻擊方的躍遷效應；該子系統S1001A可藉此以上三個單元的組合，實施為一反屏蔽機制，以避免攻擊方利用屏蔽攻擊而封鎖一般量子金鑰的遠端存取。

【0042】 此外，如圖3-2所示流程，上述屏蔽與反屏蔽模組M103之『耦合常數導出單元』U106，藉由計算攻擊方的躍遷效應發生機率，可進一步推導出一第一耦合常數；其『動能強度對應單元』U107，則根據該第一耦合常數與動能的關係，建立該耦合常數與動能強度的對應資料，並根據該對應資料所包含的動

能與位置函數的關係，可建立出波函數與動量的轉換模型，以便進一步提供該子系統S1001A透過波函數調控模組M101進行波函數調控時，所需的動量參數；該子系統S1001A可藉此以上兩個單元U106與U107的組合，實施為一屏蔽機制，經由調控量子通訊環境的系統波函數，以避免攻擊方透過量子通訊通道，偵測我方量子金鑰儲存組態的波函數。以上U103~U107五個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可整合為一屏蔽與反屏蔽模組M103，可達成先前技術未提供之避免量子金鑰的存取被封鎖以及避免量子金鑰組態的波函數被偵測之功能。

【0043】 在另一實施例中，參考圖1-2，關於本發明之量子金鑰消除子系統S1002A，為使攻擊方無法經由量子通道觀察量子金鑰消除過程中相關系統物理量的變化，需要一可改變光通訊通道之折射率的動能項，其實作包括以下模組：一『歐拉-拉格朗日變分模組』M201；一『綱量分析模組』M202；以及一『哈密頓系統轉換模組』M203。其中，歐拉-拉格朗日變分模組M201，先根據在量子通訊通道所觀測到的時間與光路徑參數，進行時間與光路徑的變分運算，並以歐拉-拉格朗日方程(Euler-Lagrange equation)的表述推導出最小作用量的穩定值；接著，綱量分析模組M202，可將該最小作用量的穩定值透過綱量，轉換為一與動量相關之表述；然後哈密頓系統轉換模組M203，可根據該動量相關之表述轉換為辛空間(或稱辛向量空間, Symplectic vector space)之廣義動量，並利用其二次型導出動能項。

【0044】 為使該子系統S1002A可進一步利用上述哈密頓系統轉換模組M203所導出的動能項，以實現其調控折射率之能力，參考圖1-2，該量子金鑰消除子系統S1002A應再實作以下模組：一『諾特定理轉換模組』M204；一『哈特

里-福克方程運算模組』M205；一『角頻率調控模組』M206；一『相位調控模組』M207；以及一『可調控光柵模組』M208。其中，諾特定理轉換模組M204，可將上述哈密頓系統轉換模組M203所導出的動能項帶入以斯萊特行列式所表示的系統波函數，經過包利矩陣的轉換運算導出系統波函數的相位模型，然後以諾特定理(Noether's theorem)基於電荷守恆與相位的規範不變性，再計算出具備一般全局對稱性之角動量守恆量；接著，哈特里-福克方程運算模組M205，可利用哈特里-福克方程式(Hartree–Fock equation)計算出打破該角動量守恆量所需的最低動能，並將該最低動能回報給該子系統S1002A；然後，該子系統S1002A可根據M205所回報的最低動能的需求，協同角頻率調控模組M206與相位調控模組M207，進行角頻率與相位的調控；最後，該子系統S1002A再協同可調控光柵模組M208，將完成角頻率與相位調控程序的光波導入以電光晶體實作的光柵元件，因角動量的守恆量被打破，使得量子通訊環境的光路徑折射率產生所需的變動。

【0045】 以上八個模組M201~M208可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可整合於一量子金鑰消除子系統S1002A，可於量子金鑰消除的過程中，利用打破一般全局對稱性之角動量守恆量，對現有光通訊環境之路徑折射率做暫時性的改變，使得攻擊方無法經由量子通道觀察量子金鑰消除過程中相關系統物理量的變化，再利用量子運算分析出量子金鑰在製備時所採用的自旋屬性。此一量子金鑰消除過程中的保護機制，為先前技術所無法達到之功效。

【0046】 參考圖1-2，在另一實施例中，為對抗針對量子金鑰回收過程所發動的量子運算攻擊(本發明實施例所稱金鑰回收，包含相關領域所指的金鑰回收、更新或輪替等相關程序)，可實作一量子金鑰回收子系統S1003A，至少包含

以下模組：一『誘罐建構模組』M301，可建構特定誘罐(Honeypot) ，用於觀察在量子金鑰回收過程中，來自他方量子運算攻擊的可能行為；以及一『微擾誘導模組』M302，可根據誘罐建構模組的運算結果，進行微擾誘導(Perturbation Induction)程序，以轉移量子金鑰回收過程中，來自他方量子運算的攻擊。

【0047】 在上述實施例中，為實現一量子誘罐機制，參考圖6所示，該誘罐建構模組M301可實作有以下單元：一『多微波產生單元』U301；一『可調控位能井單元』U302；一『角頻率配製單元』U303；一『激發態機率分析單元』U304；以及一『單頻諧波分析單元』U305。其中，該誘罐建構模組M301為了彈性且及時調整出所需的躍遷特徵與角頻率特徵，並利用各種特徵組合，以觀察量子金鑰來源在回收的過程中可能遭遇的各種不同的量子攻擊行為，故提供U301~U305等單元以實作以下機制：1)為觸發多種不同的躍遷效應，該誘罐建構模組M301可驅動該多微波產生單元U301利用多組不同共振頻率的微波產生器，與光量子作用出不同的躍遷效應；2)為控制躍遷機率的範圍，該誘罐建構模組M301可驅動該可調控位能井單元U302實作一位能井(potential well) ，利用散射與微擾程序，產生能級偏移，以便協同U301控制躍遷機率的範圍；3)為配置系統所需的角頻率，該誘罐建構模組M301可驅動該角頻率配製單元U303，將費米黃金定律(Fermi’s golden rule)運用於離散能階躍遷，根據所需的角頻率導出態密度，並搭配散射理論之玻恩近似法(Born approximation)推導出對應的散射截面與入射角度，以用於配製做為自旋屬性的角頻率；4)為判斷是否須對U302之位能井進行調控，該誘罐建構模組M301可驅動該激發態機率分析單元U304根據高能階至低能階所量測到的光電效應，估算激發態機率，分析是否需要對位能井U302進行調控以產生適用的能級偏移；以及5)為驗證U303所配製的角頻率是否適用，

該誘罐建構模組M301可驅動該單頻諧波分析單元U305，將U303所配製之角頻率以單頻諧波表達，再與量測到的躍遷機率分佈做比對分析，以判斷U303所配製的角頻率是否適用。以上U301~U305五個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可彈性且及時調整出所需的躍遷特徵與角頻率特徵，並利用各種特徵組合，以觀察量子金鑰來源在回收的過程中，可能遭遇的各種不同的量子攻擊行為。此一組合可實施於量子金鑰的發送端(或金鑰管理裝置)與接收端(或遠端通訊裝置)或於量子通道上的第三端做為惡意量子行為的收錄觀察機制，此為先前技術所無法達到之功效。

【0048】 另外，在同一實施例中，上述微擾誘導模組M302，為達到誘導轉移量子攻擊之功效，如圖6所示，包含以下單元：一『布洛赫球監控單元』U306，實作一具布洛赫球(Bloch sphere)座標體系之監視裝置，用於觀察、標定並分析來自他方的量子運算行為；一『角動量合成單元』U307，根據布洛赫球的監控分析結果，可透過誘罐建構模組M301使用不同的角頻率合成所需的角動量；以及一『諧波產生單元』U308，可產生角動量所對應的諧波，以微擾程序誘導人造原子產生偏移，可轉移來自他方的量子攻擊。以上U306~U308三個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合可彈性且及時轉移攻擊方的量子偵測行為，以避免攻擊方測得真正的量子金鑰相關資訊。此一組合可實施於量子金鑰的發送端(或金鑰管理裝置)與接收端(或遠端通訊裝置)或於量子通道上的第三端，以做為誘導移轉保護機制，此為先前技術所無法達到之功效。

【0049】 在另一實施例中，為強化對量子運算攻擊的偵測與反擊能力，上述之量子金鑰回收子系統S1003A，參考圖1-2，可再更進一步包含以下模組：一

『自旋屬性驗證模組』M303；一『量子攻擊偵測模組』M304；一『任意子波函數產生模組』M306；以及一『角動量精確性驗證模組』M305。其中，1)首先該自旋屬性驗證模組M303，導出量子自旋屬性之拓樸性質、動量性質，以及偏振性質，以分析量子是否具有特定的自旋屬性；2)接著該量子攻擊偵測模組M304，分析變形的量子運算攻擊，並根據共同基底與變化區間，協同自旋屬性驗證模組M303，以便進一步鎖定惡意的量子攻擊；3)此外該任意子波函數產生模組M306，利用任意子(anyon)的二維模型，調控角動量，以改變自旋角度循環生成多種波函數，可混淆來自他方的量子運算；以及4)同時該角動量精確性驗證模組M305，運用微擾理論，提供該子系統各單元或各模組驗證計算其角動量的精確性是否適用。藉由以上模組M303~M306之組合以支持該量子金鑰回收子系統S1003A進一步提供對量子運算攻擊的偵測與反擊機制。

【0050】 其中，上述之自旋屬性驗證模組M303，為透過偵測量子之不同自旋屬性，以做為可標定的量子系統特徵，參考圖6該模組M303包含有以下單元：一『投影量子數分析單元』U309；一『包利向量分析單元』U310；一『簡諧振子分析單元』U311；以及一『光路徑分析單元』U312。為量測與分析量子自旋屬性，以標定量子系統特徵，該自旋屬性驗證模組M303提供以下量測分析機制：首先呼叫該投影量子數分析單元U309對波函數異常的通訊環境進行分析，並協同一可實施斯特-恩革拉赫實驗(Stern-Gerlach experiment)之量測裝置，克服不確定性原理的量測限制，可測得大量粒子的自旋向量，再以自旋沿着各座標軸分量的數學期望值做為各自旋分量，推算得到多重自旋態的自旋投影量子數；接著再呼叫該包利向量分析單元U310與該簡諧振子分析單元U311以及該光路徑分析單元U312。其中，該包利向量分析單元U310將該投影量子數分析單元U309所取

得的多重態的自旋投影量子數透過包利向量(Pauli vector)與歐拉公式(Euler's formula)，可得一複平面座標做為量子自旋屬性之拓樸不變量；該簡諧振子分析單元U311分析量子系統之簡諧振子的角頻率線性組合與相位線性組合，以做為量子自旋屬性的動量特徵；以及該光路徑分析單元U312分析通訊環境之光路徑的折射率以及散射角度的組合，以做為量子自旋屬性的偏振特徵。以上U309~U312四個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之自旋屬性驗證模組M303，可整合得到量子自旋屬性之拓樸性質、動量性質，以及偏振性質，可鎖定特定自旋屬性的組合做為量子系統特徵，以驗證量子通訊環境中是否具備應該警示的量子系統特徵，此為先前技術所無法達到之功效。

【0051】 在同一實施例中，上述之量子攻擊偵測模組M304，如圖6所示，則包含有以下單元：一『角動量相容觀察單元』U313，利用哈密頓算符與角動量算符的對易關係，可量測出兩者共同本徵值的變化區間，並導出角動量與量子系統共同的本徵態；一『不相容可觀察量驗證單元』U314，可對一量子測量其哈密頓量，再對另一量子測量其角動量，若此兩種量子可觀察量之不確定性乘積無法證明其互為不相容可觀察量，則可驗證此二量子態具有共同基底；以及一『異常變動偵測單元』U315，如圖7-1所示之一實施例參考流程，U315可根據偵測通訊環境之量子系統的異常變化，將異常訊號回饋該量子金鑰回收子系統S1003A，以協同角動量相容觀察單元U313與不相容可觀察量驗證單元U314將輸出結果回報給S1003A，以進一步判斷確認是否存在可疑的變形量子攻擊。以上U313~U315三個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之量子攻擊偵測模組M304，可藉由對量子系統物

理量與角動量的觀察與分析，可測定是否存在與特定量子態具有共同基底的變形量子攻擊，可實施為量子系統的資安黑名單機制，此為先前技術所無法達到之功效。

【0052】 此外，在同一實施例中，為完備上述量子攻擊偵測模組M304之異常變動偵測單元U315，參考圖7-2，該單元U315需進一步實作以下子單元：一『異常退相干偵測子單元』U31501，可根據對量子通訊環境所偵測的退相干速率，判斷是否回饋該量子金鑰回收子系統S1003A一異常訊號；一『波函數坍縮偵測子單元』U31502，可對量子通訊環境進行波函數監控，以多次不同的測量量子系統，若量測到可能因中間人量子攻擊而導致的波函數坍縮現象，則回饋該量子金鑰回收子系統S1003A一異常訊號；一『異常躍遷偵測子單元』U31503，可根據對量子通訊環境所偵測的躍遷機率，判斷是否回饋該量子金鑰回收子系統S1003A一異常訊號；一『異常變數偵測子單元』U31504，導入EPR悖論(Einstein-Podolsky-Rosen paradox)分析程序，若偵測到量子通訊環境的一量子物理行為同時符合定域實在論(locality-realism theory)與不確定原理(uncertainty principle)，表示可能存在異常環境變數，則回饋該量子金鑰回收子系統S1003A一異常訊號；以及一『異常熵變動偵測子單元』U31505，可根據偵測通訊環境之量子系統的熵(entropy)變化程度，判斷是否回饋該量子金鑰回收子系統S1003A一異常訊號。以上U31501~U31505五個子單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之異常變動偵測單元U315，可藉由監控量子通訊環境的系統變化，有效示警通訊環境中異常的量子行為，此為先前技術所無法達到之功效。

【0053】 另外，在同一實施例中，有關上述量子金鑰回收子系統S1003A之角動量精確性驗證模組M305，如圖6所示，則進一步包含有以下單元：一『零微擾波函數計算單元』U316，利用零微擾哈密頓量、總角動量平方、軌道角動量平方以及自旋角動量平方等四個算符(H_0, J^2, L^2, S^2)的共同本徵函數做為零微擾波函數，可計算出一階能量位移；以及一『能量位移驗證單元』U317，先以可交換運算子完備集 (Complete set of commuting observables，C.S.C.O.)處理可能因能級簡併導致的固有值退化問題，然後再將量測到的簡諧振子週期函數進行傅立葉展開程序(Fourier Expansion) ，而導出諧波關係，再透過計算諧波的變化，測得能級偏移，最後再利用計算出的一階能量位移與量測到的能級偏移作比對，以確認估算出的角動量其精確性是否適用。以上U316與U317兩個單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之角動量精確性驗證模組M305，藉由搭配微擾理論的實作，可提升角動量估算的精度，除可確保角動量可做為依據本發明實施例之系統重要的內稟屬性(intrinsic property)外；參考圖8顯示M305於依據本發明實施例之系統之支援關係，對於量子金鑰回收子系統S1003A之微擾誘導模組M302，亦可同時提升其角動量合成的準確性；此外亦可支援依據本發明實施例之量子金鑰消除子系統S1002A在諾特定理轉換模組M204實施諾特定理轉換時，確保其所導出的角動量守恆量之正確性；除了正確性的考量外，本驗證模組M305亦可協助依據本發明實施例之量子金鑰回收子系統S1003A以微擾誘導模組M302實施微擾誘導程序時，進行一級或二級能量與波函數的微擾修正，以確保微擾誘導程序的能級偏移符合需求；最重要的是，若角動量計算的誤差過大，造成簡諧振子分析單元U311的線性分析有

所偏差，亦可能影響上述自旋屬性驗證模組M303的判斷結果，故此模組M305對維護整個系統的警示機制亦有關鍵作用；以上皆為先前技術未實施之功效。

【0054】 參考圖7-2，在一些實施例中，為進一步降低上述角動量精確性驗證模組M305之驗證誤差，該模組之能量位移驗證單元U317可再包含以下子單元：一『簡併能階分析子單元』U31701；一『質量干擾分析子單元』U31702；以及一『蘭姆位移測定子單元』U31703。該能量位移驗證單元U317提供以下分析模式以降低能級偏移的量測誤差：1)驅動該簡併能階分析子單元U31701，利用對自旋量子數的狀態分析，可促進判斷目前的能量位移是否為一簡併態；2)驅動該質量干擾分析子單元U31702，利用分析質量解析度，可判斷目前的能量位移是否存在質量干擾；以及3)若能量位移量測的結果可確認為簡併態且存在質量干擾，則驅動該蘭姆位移測定子單元U31703用蘭姆位移(Lamb shift)之計算進行能級偏移分析。以上U31701~U31703三個子單元可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然此組合之能量位移驗證單元U317，可在能量位移受到簡併態與質量干擾的影響下，仍可維護角動量計算的精確性，此為先前技術所無法達到之功效。

【0055】 參考圖1-2，在另外一些實施例中，為加強本發明實施例在量子金鑰回收過程對相關量子運算攻擊的反制能力，其量子金鑰回收子系統S1003A可再進一步包含以下模組：一『重送攻擊回應模組』M307；一『量子亂數產生模組』M308；一『前像攻擊模組』M309；一『第二前像攻擊模組』M310；以及一『碰撞攻擊模組』M311。其中，1)該重送攻擊回應模組M307，首先回應攻擊方所發動的重送攻擊(replay attack)；2)該量子亂數產生模組M308產生一偽造的雜湊值(hash value)或訊息摘要(digest)，以便支援M307接著使用偽造的應答封包

(acknowledge)、偽造的封包檔頭(package header)以及偽造的封包填塞(package padding)回應重送攻擊；3)該前像攻擊模組M309採用偽造的雜湊函式(hash function))搭配真實的訊息摘要，進一步對攻擊方發動前像攻擊(preimage attack)；4)該第二前像攻擊模組M310隱藏真實的雜湊函式，並改變真實訊息摘要的長度，再用以對攻擊方發動第二前像攻擊(second-preimage attack)；以及5)該碰撞攻擊模組M311以真實雜湊函式的反函式做為雜湊函式，以真實訊息摘要的反元素作為訊息摘要，最終用以對攻擊方發動多碰撞攻擊(multi-collision attack)。藉由以上模組M307~M311之組合以支持該量子金鑰回收子系統S1003A在金鑰回收階段針對可能遭遇以量子運算為技術手段對金鑰驗證程序所發動的攻擊，提供反制機制。以上M307~M311五個模組可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然而對於在量子金鑰回收過程中試圖攔截相關交換訊息的攻擊方，此組合可對其實施基本且有效的反制機制，以避免攻擊方蒐集足夠多的交握訊息而進行破密分析，此為先前技術所無法達到之功效。

【0056】 最後，參考圖1-2，在上述實施例中，為再增加本發明實施例在量子金鑰回收過程對持續性的量子運算攻擊的進階反制能力，其量子金鑰回收子系統S1003A可再進一步包含以下模組：一『偽金鑰攻擊模組』M312；一『偽量子態攻擊模組』M313；以及一『量子阻斷服務攻擊模組』M314。其中，1)該偽金鑰攻擊模組M312首先對攻擊方發送假造的公開金鑰；2)該偽量子態攻擊模組M313接著使用不正確的自旋屬性組合，以產製大量偽造的量子態；以及3)該量子阻斷服務攻擊模組M314而後以阻斷服務(DoS)的攻擊型態，對攻擊方發送大量的退相干組態。藉由以上模組M312~M314之組合以支持該量子金鑰回收子系統S1003A在金鑰回收階段針對可能遭遇以量子運算為技術手段對交握訊息所發動

的攻擊，提供進階反制機制。以上M312~M314三個模組可基於相關之習知技術而實現為軟體單元、硬體單元或以軟體結合方式實現，然而對於在量子金鑰回收過程中持續性蒐集相關交換訊息的攻擊方，此組合可對其實施進階反制機制，可迅速且有效地消耗攻擊方的量子運算資源，進而癱瘓其在成本考量下有限的量子算力，此為先前技術所無法達到之功效。

【0057】 藉此，上述本發明的多個實施例可實現對抗量子運算攻擊的金鑰管理機制，可在量子金鑰儲存、量子金鑰消除，以及量子金鑰回收等不同金鑰管理階段，提供一般量子金鑰管理系統完整的對抗架構。此技術可實現為高強度的抗量子運算之金鑰管理裝置或系統，且可實現於欲進行量子通訊的發送端與接收端。在一些實施例中，此技術可視系統的資安需求，除了可偵測量子攻擊與迴避量子攻擊之外，還能夠進一步選擇是否實施基本或進階的攻擊反制模組。此外，此系統之相關技術手段皆能透過具合理成本之裝置實現，有效克服現行多數PQC方案須透過高昂成本之設備運作的瓶頸，同時也提供了多數先前技術在現行PQC方案所無法支援量子金鑰管理系統的資安機制。

【0058】 本發明在上文中已以多個實施例揭露，然熟習本項技術者應理解的是，該實施例僅用於描繪本發明，而不應解讀為限制本發明之範圍。應注意的是，舉凡與該實施例等效之變化與置換，以及本發明所揭露之相關元件於同等實施領域之重組，均應設為涵蓋於本發明之範疇內。因此，本發明之保護範圍當以申請專利範圍所界定者為準。

【符號說明】

【0059】

10	遠端裝置
20	金鑰管理裝置
100、200	通訊模組
LK	通訊連結
S1000	系統
S1000A	用於金鑰管理機制的抗量子運算之系統
S1001	第一子系統
S1001A	量子金鑰儲存子系統
S1002	第二子系統
S1002A	量子金鑰消除子系統
S1003	第三子系統
S1003A	量子金鑰回收子系統
M101	波函數調控模組
M102	系統波函數分析模組
M103	屏蔽與反屏蔽模組
M201	歐拉-拉格朗日變分模組
M202	綱量分析模組
M203	哈密頓系統轉換模組
M204	諾特定理轉換模組
M205	哈特里-福克方程運算模組
M206	角頻率調控模組
M207	相位調控模組

M208	可調控光柵模組
M301	誘罐建構模組
M302	微擾誘導模組
M303	自旋屬性驗證模組
M304	量子攻擊偵測模組
M305	角動量精確性驗證模組
M306	任意子波函數產生模組
M307	重送攻擊回應模組
M308	量子亂數產生模組
M309	前像攻擊模組
M310	第二前像攻擊模組
M311	碰撞攻擊模組
M312	偽金鑰攻擊模組
M313	偽量子態攻擊模組
M314	量子阻斷服務攻擊模組
U101	量子系統量測單元
U10101	二次量子化計算子單元
U10102	GW 近似法計算子單元
U10103	WKB 近似法計算子單元
U10104	變分近似法計算子單元
U102	系統波函數分析單元
U10201	斯萊特行列式計算子單元

U10202	包利矩陣轉換子單元
U10203	玻恩定則運算子單元
U10204	法蘭克-康登原理分析子單元
U10205	絕熱近似運算子單元
M10201	射影計算子模組
M10202	福克空間轉換子模組
M10203	希爾伯特變換子模組
M10204	二次量子化子模組
M10205	傅立葉轉換子模組
M10206	泛函分析子模組
M10207	歸一化運算子模組
M10208	總均計算子模組
M10209	薛丁格方程轉換子模組
U103	角動量耦合單元
U104	自旋軌道耦合單元
U105	重原子效應產生單元
U106	耦合常數導出單元
U107	動能強度對應單元
U301	多微波產生單元
U302	可調控位能井單元
U303	角頻率配製單元
U304	激發態機率分析單元

U305	單頻諧波分析單元
U306	布洛赫球監控單元
U307	角動量合成單元
U308	諧波產生單元
U309	投影量子數分析單元
U310	包利向量分析單元
U311	簡諧振子分析單元
U312	光路徑分析單元
U313	角動量相容觀察單元
U314	不相容可觀察量驗證單元
U315	異常變動偵測單元
U31501	異常退相干偵測子單元
U31502	波函數坍縮偵測子單元
U31503	異常躍遷偵測子單元
U31504	異常變數偵測子單元
U31505	異常熵變動偵測子單元
U316	零微擾波函數計算單元
U317	能量位移驗證單元
U31701	簡併能階分析子單元
U31702	質量干擾分析子單元
U31703	蘭姆位移測定子單元

【發明申請專利範圍】

【請求項1】一種用於金鑰管理機制的抗量子運算之系統，該系統至少包括一第一子系統，可用於對抗針對量子金鑰儲存階段所進行的量子運算攻擊，其中該第一子系統包含：

一波函數調控模組，用以運用薛丁格方程式藉由動量調整而改變波函數；

一系統波函數分析模組，用以經由絕熱近似的計算機制，估計出他方量子運算所使用的波函數；以及

一屏蔽與反屏蔽模組，用以避免儲存中的量子金鑰受到他方量子運算的偵測或封鎖，該屏蔽與反屏蔽模組包含：

一角動量耦合單元，用於耦合出所需的自旋角動量；

一自旋軌道耦合單元，採用j-j耦合程序，以進行軌道與自旋角動量的耦合；

一重原子效應產生單元，經由增強自旋軌道的耦合效應，以進一步激發躍遷效應；

一耦合常數導出單元，藉由計算躍遷效應之發生機率，以進一步推導出耦合常數；以及

一動能強度對應單元，用以根據耦合常數與動能的關係，建立耦合常數與動能強度的對應資料；

其中該第一子系統係配置為根據該系統波函數分析模組的計算結果，判斷量子通訊環境是否存在異常的量子系統波函數，以決定是否呼叫該屏蔽與反屏蔽模組啟動屏蔽或反屏蔽機制，並透過該波函數調控模組進行波函數的調控。

【請求項2】如請求項1所述之系統，其中該系統進一步包括一第二子系統，在完成該量子金鑰儲存階段之後，用於對抗針對量子金鑰消除程序所進行的量子運算攻擊，並根據導出的動能調整光路徑的折射率，該第二子系統包含：

一歐拉-拉格朗日變分模組，用以進行時間與光路徑的變分運算，並以歐拉-拉格朗日的表述推導出最小作用量的穩定值；

一綱量分析模組，用以將該歐拉-拉格朗日變分模組所導出之最小作用量透過綱量，轉換為一與動量相關之表述；以及

一哈密頓系統轉換模組，用以根據該綱量分析模組轉換得出之與動量相關之表述轉換為辛空間之廣義動量，並利用該廣義動量之二次型導出用於調整光路徑折射率的動能項。

【請求項3】如請求項2所述之系統，其中該系統進一步包括一第三子系統，在完成該量子金鑰儲存階段之後，用於對抗針對量子金鑰回收流程所進行的量子運算攻擊，該第三子系統至少包含：

一誘罐(Honeypot)建構模組，用以建構特定誘罐，觀察在量子金鑰回收過程中來自他方量子運算攻擊的可能行為，以避免系統於量子金鑰回收流程受到他方量子運算的攻擊，該誘罐建構模組包含：

一多微波產生單元，用以利用多組不同共振頻率的微波產生器，與光量子作用出不同的躍遷效應；

一可調控位能井(potential well)單元，用於利用散射與微擾程序，產生能級偏移，以便控制該多微波產生單元所觸發之躍遷效應其躍遷機率的範圍；

一角頻率配製單元，用於將費米黃金定律(Fermi’s golden rule)運用於該可調控位能井單元所調控之離散能階躍遷，根據所需的角頻率導

出態密度，並搭配散射理論之玻恩近似法推導出對應的散射截面與入射角度，以用於配製做為自旋屬性的角頻率；

一激發態機率分析單元，用於根據高能階至低能階所量測到的光電效應，估算激發態機率，分析是否需要利用該可調控位能井單元進行調控；以及

一單頻諧波分析單元，用於將該角頻率配製單元所配製之做為自旋屬性的角頻率以單頻諧波表達，再與量測到的躍遷機率分佈做比對分析，以驗證所配製的角頻率是否適用；以及

一微擾誘導模組，用於根據該誘罐建構模組的運算結果，當該誘罐建構模組觀察到來自他方量子運算攻擊的可能行為時，進行微擾誘導程序，以轉移量子金鑰回收過程中，來自他方量子運算的攻擊，該微擾誘導模組包含：

一布洛赫球監控單元，用於標定及分析來自他方的量子運算行為；

一角動量合成單元，根據該布洛赫球監控單元的分析結果，透過該誘罐建構模組使用不同的角頻率合成所需的角動量；

一諧波產生單元，用於產生該角動量合成單元所合成的角動量所對應的諧波，以微擾程序誘導人造原子產生偏移，可轉移來自他方的量子攻擊。

【請求項4】如請求項2所述之系統，其中該系統進一步包括一第三子系統，在完成該量子金鑰儲存階段之後，用於對抗針對量子金鑰回收流程所進行的量子運算攻擊，該第三子系統至少包含：

一自旋屬性驗證模組，用於導出量子自旋屬性之拓樸性質、動量性質，以及偏振性質，以分析量子是否具有特定的自旋屬性；

一量子攻擊偵測模組，用於分析變形的量子運算攻擊，並根據共同基底與變化區間，協同該自旋屬性驗證模組，以進一步鎖定惡意的量子攻擊；

一角動量精確性驗證模組，用以運用微擾理論，提供該第一子系統、該第二子系統及該第三子系統中至少一者驗證計算角動量的精確性是否適用；以及

一任意子(anyon)波函數產生模組，用於在該量子攻擊偵測模組協同該自旋屬性驗證模組鎖定惡意的量子攻擊之後，利用任意子的二維模型，調控角動量，以改變自旋角度循環生成多種波函數，從而混淆來自他方的量子運算。

【請求項5】如請求項1所述之系統，其中為了導出一量子系統之波函數之近似解，該第一子系統之系統波函數分析模組包含：

一斯萊特行列式計算子單元，用以將多個波函數量測結果轉換成斯萊特行列式(Slater determinant)的形式；

一包利矩陣轉換子單元，用以將該斯萊特行列式轉換成多個包利矩陣以表達多個觀測值；

一玻恩定則運算子單元，用以利用玻恩定則推算該包利矩陣轉換子單元所表述之各觀測值的對應躍遷機率；

一法蘭克-康登原理(Franck-Condon principle)分析子單元，用於運用法蘭克-康登原理的量子力學公式，將該玻恩定則運算子單元所推算出的躍遷機率與一量子諧振子函數進行分析，以導出量子波函數與核波函數的近似解；以及

一絕熱近似運算子單元，用於利用該法蘭克-康登原理分析子單元所導出的量子波函數與核波函數的近似解以絕熱近似運算以得到一整體波函數之近似解。

【請求項6】如請求項1所述之系統，其中該第一子系統之系統波函數分析模組，為增進量子攻擊之量測能力，進一步包含：

一二次量子化計算子單元，用於量測計算經過二次量子化所發動的諧振子攻擊；

一GW近似法計算子單元，具備GW近似計算與微擾運算能力，用於量測激發態的攻擊或是無法進行泛函分析的量子攻擊；

一WKB近似法計算子單元，用於量測波函數變化緩慢的量子攻擊；以及

一變分近似法計算子單元，透過泛函分析的變分法，用於量測波函數變化快速的量子攻擊；

其中，該系統波函數分析模組對於無法判斷量子攻擊屬性來自於玻色子還是費米子的狀況則呼叫該二次量子化計算子單元使用創生與湮滅算符(creation and annihilation operators)進行諧振子分析；對於因利用遮蔽效應而無法進行泛函分析的量子攻擊或是激發態的量子攻擊，該系統波函數分析模組則呼叫該GW近似法計算子單元使用GW近似法做量測計算；對於對波函數變化緩慢的量子攻擊，該系統波函數分析模組則呼叫該WKB近似法計算子單元以WKB近似法進行推估量測；對於波函數變異快速的量子攻擊，該系統波函數分析模組則呼叫該變分近似法計算子單元透過泛函分析的變分法進行推估量測。

【請求項7】如請求項1所述之系統，其中該第一子系統之系統波函數分析模組之絕熱近似運算子單元，為將多個波函數量測所導出的結果，表示為一初始平衡態以便進行絕熱近似運算，進一步包含：

一射影計算子模組，用於利用射影算子，推估所量測的量子系統之量子比特的線性組合；

一福克空間(Fock Space)轉換子模組，用於將該射影計算子模組所推估之量子比特的線性組合以福克空間的奇異積分算子表示為一量子系統態；

一希爾伯特變換子模組，用於將該福克空間轉換子模組所表述之福克空間的量子系統態轉換至多維度的希爾伯特空間；

一二次量子化子模組，用於利用創生與湮滅算符對該希爾伯特變換子模組所表述之希爾伯特空間的量子系統態進行二次量子化，二次量子化之結果用於描述量子系統的哈密頓量；

一傅立葉轉換子模組，用於將該二次量子化子模組所表述之量子系統的哈密頓量進行傅立葉轉換，以消除包含位置與動量之物理量的不確定性，以得到轉換後的系統物理量；

一泛函分析子模組，用於利用變分法對該傅立葉轉換子模組所得出的已確定的轉換後的系統物理量做分析，以獲得可代表波函數特性的機率分布；

一歸一化運算子模組，用於將該泛函分析子模組所導出的一機率分布進行歸一化程序；

一總均計算子模組，用於根據該歸一化運算子模組所導出的已歸一化的機率分布估計總體均值；以及

一薛丁格方程轉換子模組，用於根據該總均計算子模組所估計的總體均值、該泛函分析子模組所導出的機率分布，以及該傅立葉轉換子模組所得出的已確定的轉換後的系統物理量，將此量子系統態以一時間相關的薛丁格方程式表示，以做為絕熱近似運算所需的初始平衡態。

【請求項8】如請求項2所述之系統，其中該第二子系統，為實現其調控折射率之能力，進一步包含：

一諾特定理轉換模組，用於根據一動能項以諾特定理轉換為具備一般全局對稱性之角動量守恆量；

一哈特里-福克方程運算模組，用於根據該諾特定理轉換模組之轉換結果，計算打破守恆性所需的最低動能；

一角頻率調控模組，用於根據該哈特里-福克方程運算模組所計算得出之最低動能的需求，進行角頻率的調控程序；

一相位調控模組，用於根據該哈特里-福克方程運算模組所計算得出之最低動能的需求，進行相位的調控程序；以及

一可調控光柵模組，用於將完成角頻率與相位調控程序的光波導入以電光晶體實作的光柵元件，因角動量的守恆量被打破，使得折射率產生所需的變動。

【請求項9】如請求項4所述之系統，其中該第三子系統之自旋屬性驗證模組，包含：

一投影量子數分析單元，用以分析得到多重自旋態的自旋投影量子數；

一包利向量(Pauli vector)分析單元，用於將該投影量子數分析單元所得出的多重自旋態的自旋投影量子數透過包利向量與歐拉公式，以得到一複平面座標做為量子自旋屬性之拓樸不變量；

一簡諧振子分析單元，用於分析量子系統之簡諧振子的角頻率線性組合與相位線性組合，以做為量子自旋屬性的動量特徵；以及

一光路徑分析單元，用於分析光路徑的折射率以及散射角度的組合，以做為量子自旋屬性的偏振特徵；

其中，該自旋屬性驗證模組藉由該投影量子數分析單元與該包利向量分析單元得到量子自旋屬性之拓樸性質，並藉由該簡諧振子分析單元得到量子自旋屬性之動量性質，同時藉由該光路徑分析單元得到量子自旋屬性之偏振性質，以助於鎖定特定自旋屬性的組合，以驗證量子通訊環境中是否具備應該警示的量子系統特徵。

【請求項10】如請求項4所述之系統，其中該第三子系統之量子攻擊偵測模組，包含：

一角動量相容觀察單元，用於利用哈密頓算符與角動量算符的對易關係，量測出該哈密頓算符與該角動量算符的共同本徵值的變化區間，並導出對應的共同的本徵態；

一不相容可觀察量驗證單元，用於測量一第一量子的哈密頓量，再測量一第二量子的角動量，若該第一量子及該第二量子可觀察量之不確定性乘積無法證明該第一量子及該第二量子互為不相容可觀察量，則可驗證該第一量子及該第二量子之量子態具有共同基底；以及

一異常變動偵測單元，用於根據偵測通訊環境之量子系統的異常變化，回饋該第三子系統，以協同該角動量相容觀察單元與該不相容可觀察量驗證單元確認是否存在可疑的量子攻擊；

其中，該異常變動偵測單元將偵測到量子系統的異常變化回饋給第三子系統，再由該第三子系統利用該角動量相容觀察單元以取得偵測到的角動量與量子系統的共同本徵態，該第三子系統同時利用該不相容可觀察量驗證單元以判斷偵測到的量子態與特定量子態是否具有共同基底，以助於該第三子系統確認是否存在可疑的變形量子攻擊。

【請求項11】如請求項4所述之系統，其中該第三子系統之角動量精確性驗證模組，包含：

一零微擾波函數計算單元，用於利用零微擾哈密頓量、總角動量平方、軌道角動量平方以及自旋角動量平方之算符的共同本徵函數做為零微擾波函數，計算出一階能量位移；以及

一能量位移驗證單元，用於利用該零微擾波函數計算單元所計算出的一階能量位移與量測到的能級偏移作比對，以確認估算出的角動量之精確性是否適用。

【請求項12】如請求項11所述之系統，其中該能量位移驗證單元為進一步降低驗證誤差，包含：

一簡併能階分析子單元，用於利用對自旋量子數的狀態分析，判斷目前的能量位移是否為一簡併態；

一質量干擾分析子單元，用於利用分析質量解析度，判斷目前的能量位移是否存在質量干擾；以及

一蘭姆位移測定子單元，用於當能量位移量測的結果確認為簡併態或存在質量干擾時，採用蘭姆位移之計算進行能級偏移分析；

其中，該能量位移驗證單元先藉由該簡併能階分析子單元以及該質量干擾分析子單元判斷目前的能量位移量測的結果是否存在因簡併態或質量干擾所造成的誤差；若存在因簡併態或質量干擾所造成的誤差則藉由該蘭姆位移測定子單元進行能級偏移分析，以進一步降低能級偏移的量測誤差。

【請求項13】如請求項4所述之系統，其中該第三子系統為增進對量子攻擊的反擊能力，進一步包含：

一重送攻擊回應模組，用於回應攻擊方所發動的重送攻擊；

一量子亂數產生模組，用於產生一偽造的雜湊值或訊息摘要；

一前像攻擊模組，用於採用偽造的雜湊函式搭配真實的訊息摘要，以對攻擊方發動前像攻擊；

一第二前像攻擊模組，用於隱藏真實的雜湊函式，並改變真實訊息摘要的長度，以對攻擊方發動第二前像攻擊；以及

一碰撞攻擊模組，用於利用真實雜湊函式的反函式做為雜湊函式，及真實訊息摘要的反元素作為訊息摘要，以對攻擊方發動多碰撞攻擊；

其中，該第三子系統藉由該重送攻擊回應模組以及該量子亂數產生模組回應一重送攻擊；並且藉由該前像攻擊模組對攻擊方發動前像攻擊；並且藉由該第二前像攻擊模組對攻擊方發動第二前像攻擊；同時藉由該碰撞攻擊模組對攻擊方發動多碰撞攻擊，以助於增進該第三子系統對量子攻擊的反擊能力。

【請求項14】如請求項4所述之系統，其中該第三子系統為增進對量子攻擊的反擊能力，進一步包含：

一偽金鑰攻擊模組，用於對攻擊方發送假造的公開金鑰；

一偽量子態攻擊模組，用於使用不正確的自旋屬性組合，產製大量偽造的量子態；以及

一量子阻斷服務(DoS)攻擊模組，用以對攻擊方發動大量的退相干組態攻擊；

其中，當一量子金鑰在金鑰回收階段遭遇以量子運算為技術手段對交握訊息所發動的攻擊時，該第三子系統藉由利用該偽金鑰攻擊模組、該偽量子態攻擊模組以及該量子阻斷服務(DoS)攻擊模組以助於快速消耗攻擊方的量子運算資源。

【請求項15】如請求項10所述之系統，其中該量子攻擊偵測模組之異常變動偵測單元包含：

一異常退相干偵測子單元，用於根據對量子通訊環境所偵測的退相干速率，判斷是否回饋該第三子系統一異常訊號；

一波函數坍縮偵測子單元，用於對量子通訊環境進行波函數監控，若偵測到波函數坍縮現象，則回饋該第三子系統一異常訊號；

一異常躍遷偵測子單元，用於根據對量子通訊環境所偵測的躍遷機率，判斷是否回饋該第三子系統一異常訊號；

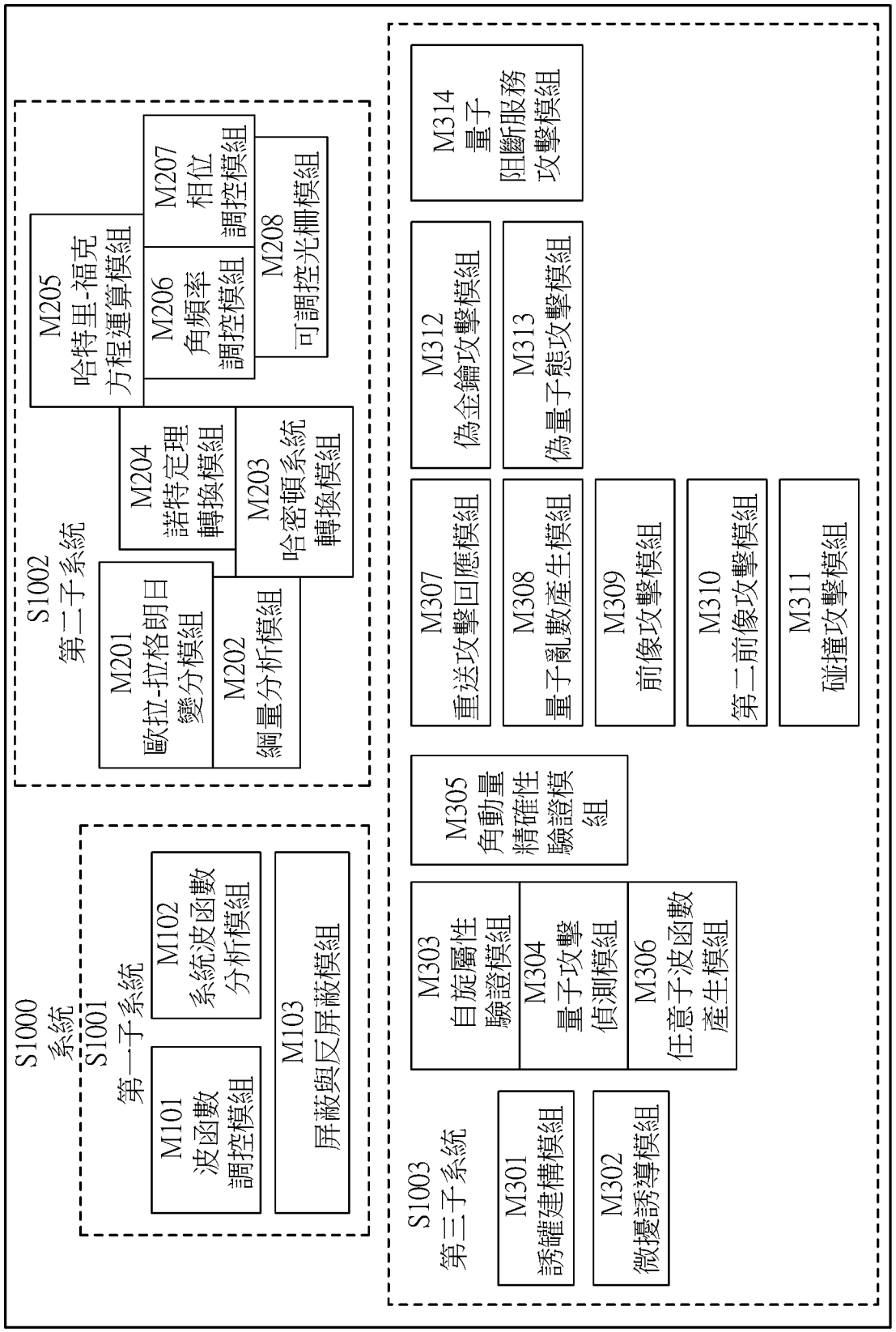
一異常變數偵測子單元，用於導入EPR悖論(Einstein-Podolsky-Rosen paradox)分析程序，若偵測到量子通訊環境的一量子物理行為同時符合定域實在論與不確定原理，則回饋該第三子系統一異常訊號；以及

一異常熵(entropy)變動偵測子單元，可根據偵測通訊環境之量子系統的熵變化程度，判斷是否回饋該第三子系統一異常訊號；

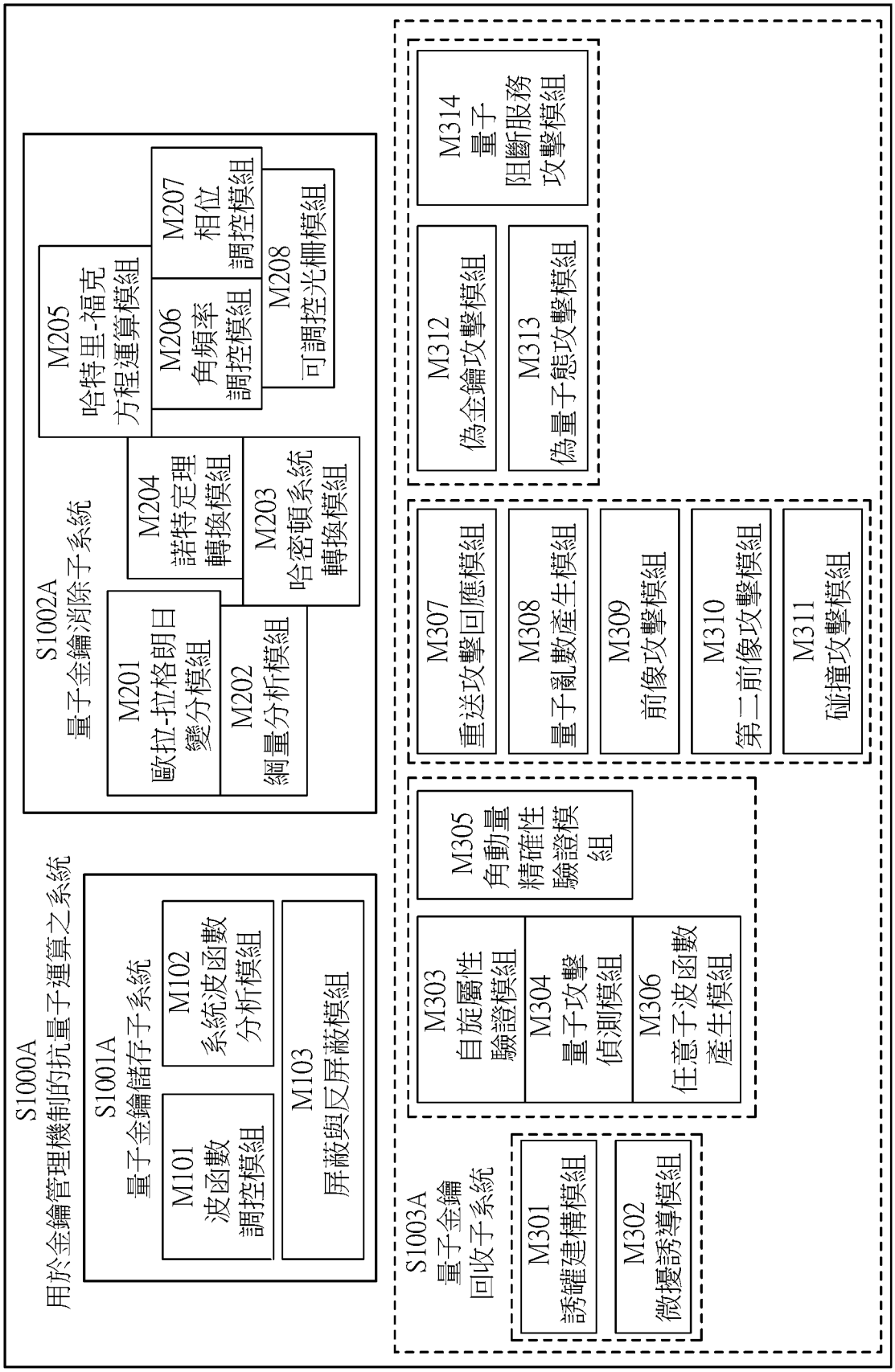
其中，該異常變動偵測單元藉由該異常退相干偵測子單元、該波函數坍縮偵測子單元、該異常躍遷偵測子單元、該異常變數偵測子單元，以及該異常熵變動

偵測子單元監控量子通訊環境的系統變化，以助於該第三子系統有效示警通訊環境中異常的量子行為。

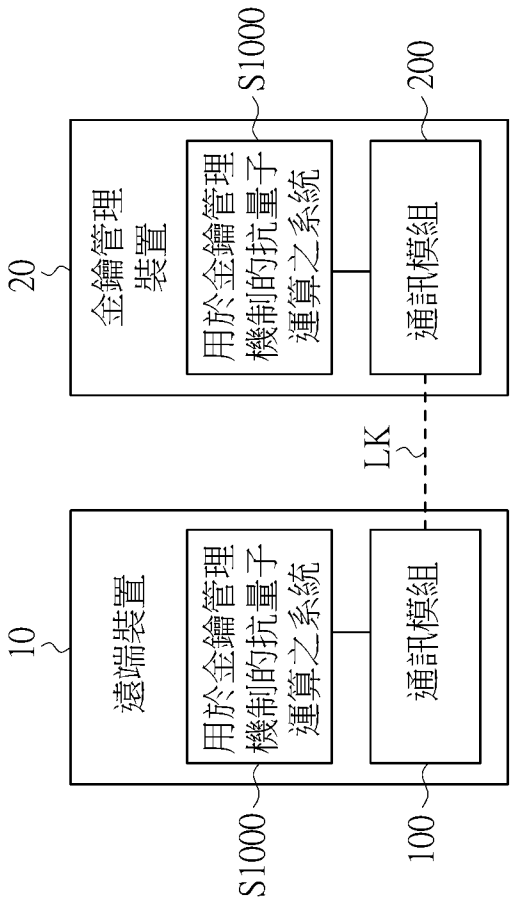
【發明圖式】


S1000
系統
S1001
第一子系統
M101
波函數
調控模組
M102
系統波函數
分析模組
M103
屏蔽與反屏蔽模組
S1002
第二子系統
M201
歐拉-拉格朗日
變分模組
M202
綱量分析模組
M203
哈密頓系統
轉換模組
M204
諾特定理
轉換模組
M205
哈特里-福克
方程運算模組
M206
角頻率
調控模組
M207
相位
調控模組
M208
可調控光柵模組
S1003
第三子系統
M301
誘罐建構模組
M302
微擾誘導模組
M303
自旋屬性
驗證模組
M304
量子攻擊
偵測模組
M306
任意子波函數
產生模組
M305
角動量
精確性
驗證模組
M307
重送攻擊回應模組
M308
量子亂數產生模組
M309
前像攻擊模組
M310
第二前像攻擊模組
M311
碰撞攻擊模組
M312
偽金鑰攻擊模組
M313
偽量子態攻擊模組
M314
量子
阻斷服務
攻擊模組

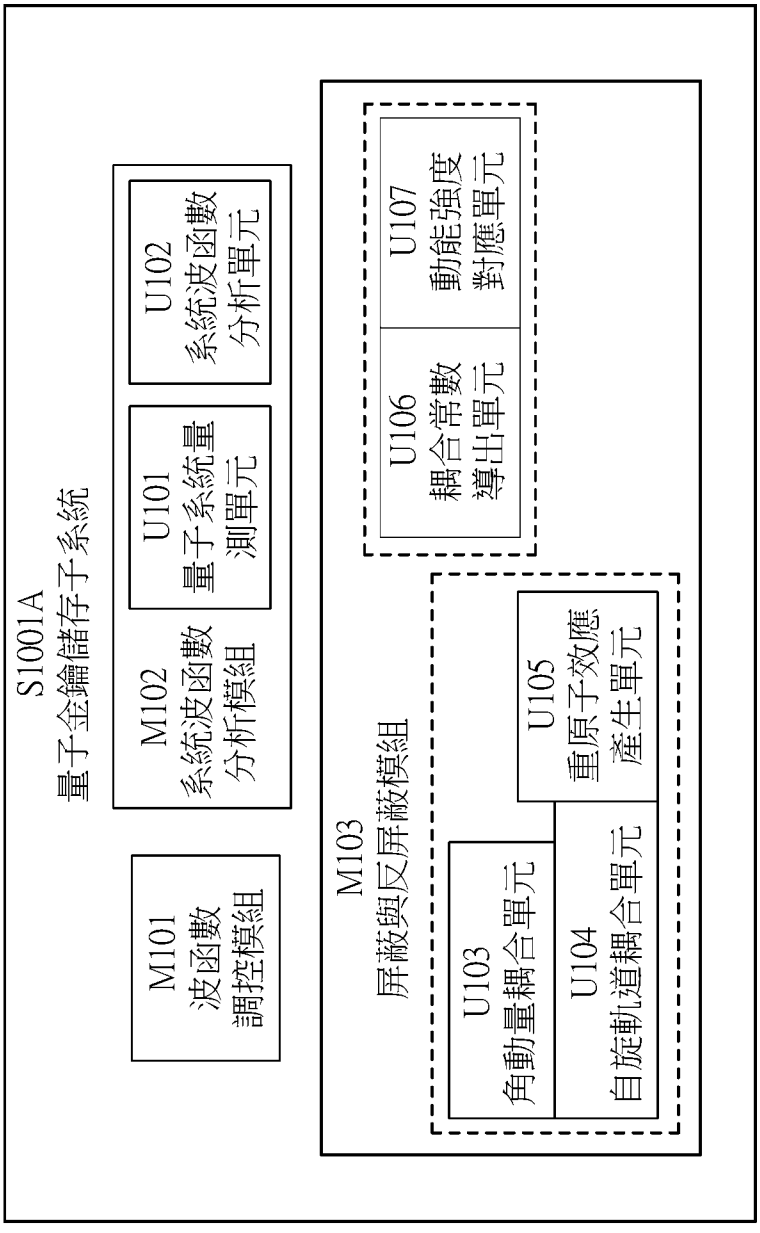
【圖1-1】


S1000A
用於金鑰管理機制的抗量子運算之系統
S1001A
量子金鑰儲存子系統
M101
波函數
調控模組
M102
系統波函數
分析模組
M103
屏蔽與反屏蔽模組
S1002A
量子金鑰消除子系統
M201
歐拉-拉格朗日
變分模組
M202
綱量分析模組
M203
哈密頓系統
轉換模組
M204
諾特定理
轉換模組
M205
哈特里-福克
方程運算模組
M206
角頻率
調控模組
M207
相位
調控模組
M208
可調控光柵模組
S1003A
量子金鑰
回收子系統
M301
誘罐建構模組
M302
微擾誘導模組
M303
自旋屬性
驗證模組
M304
量子攻擊
偵測模組
M305
角動量
精確性
驗證模組
M306
任意子波函數
產生模組
M307
重送攻擊回應模組
M308
量子亂數產生模組
M309
前像攻擊模組
M310
第二前像攻擊模組
M311
碰撞攻擊模組
M312
偽金鑰攻擊模組
M313
偽量子態攻擊模組
M314
量子
阻斷服務
攻擊模組

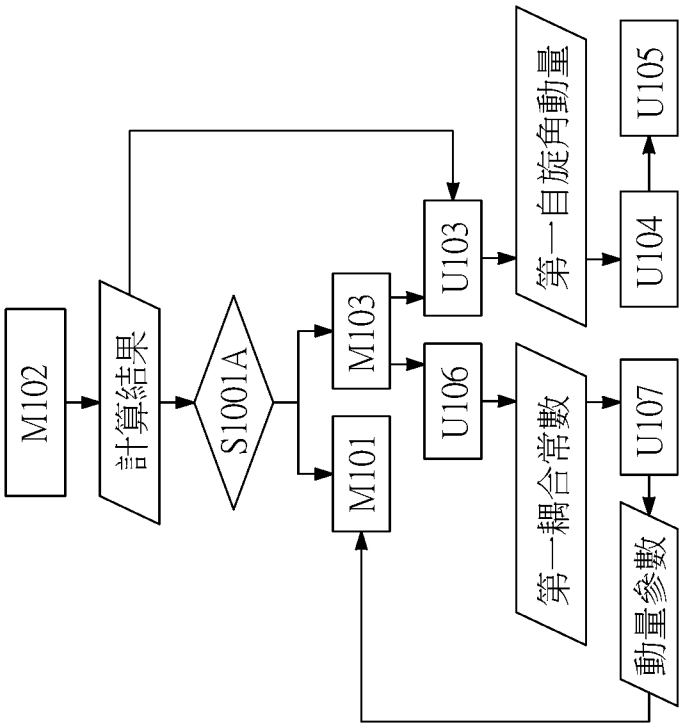
【圖1-2】


10
遠端裝置
用於金鑰管理機制的抗量子運算之系統
通訊模組
S1000
100
LK
20
金鑰管理裝置
用於金鑰管理機制的抗量子運算之系統
通訊模組
S1000
200

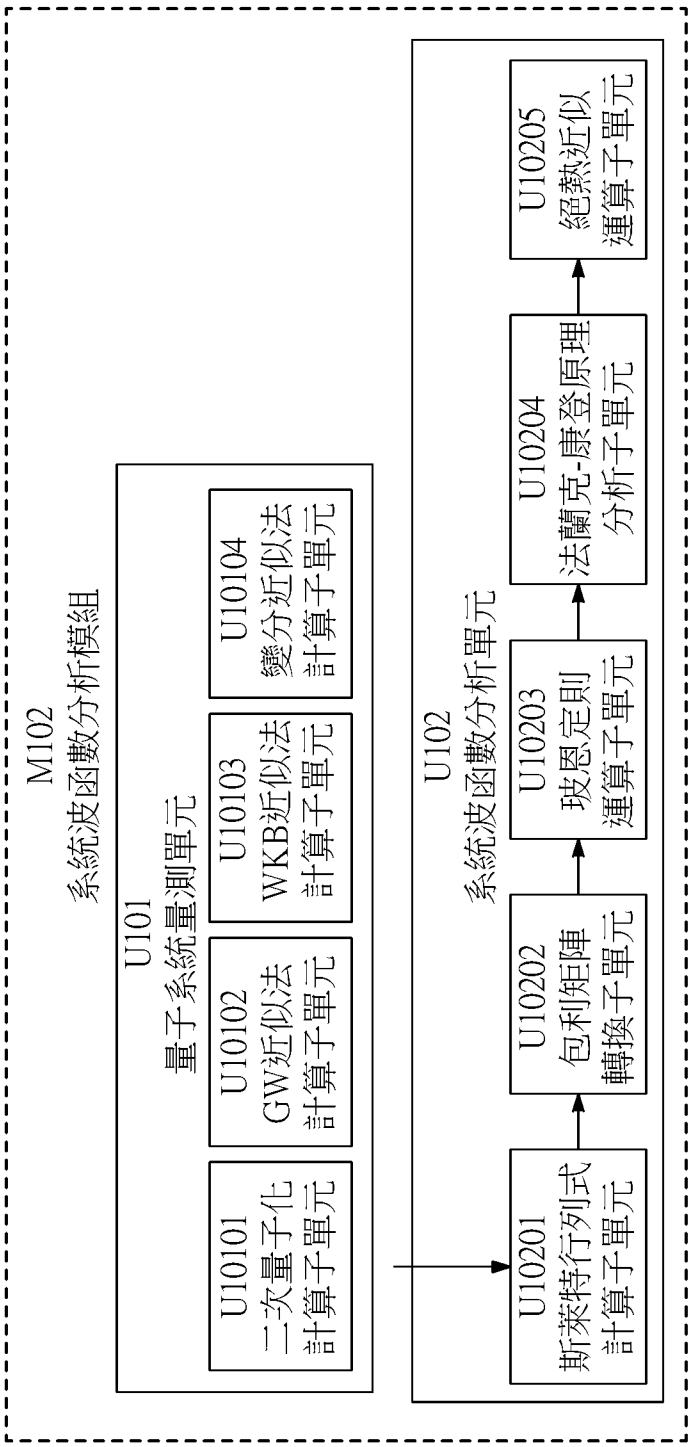
【圖2】


S1001A
量子金鑰儲存子系統
M101
波函數
調控模組
M102
系統波函數
分析模組
U101
量子系統量
測單元
U102
系統波函數
分析單元
M103
屏蔽與反屏蔽模組
U103
角動量耦合單元
U104
自旋軌道耦合單元
U105
重原子效應
產生單元
U106
耦合常數
導出單元
U107
動能強度
對應單元

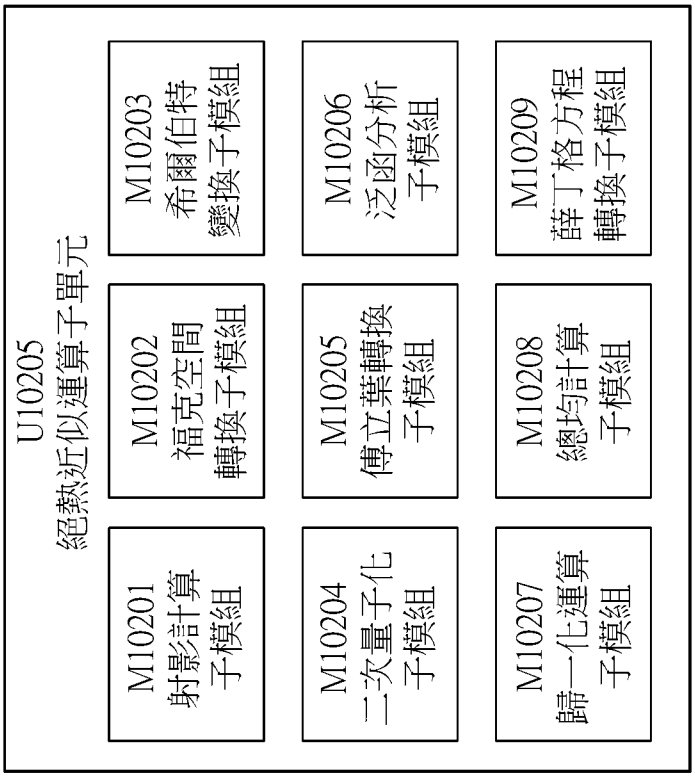
【圖3-1】


M102
計算結果
S1001A
M101
M103
U106
U103
第一耦合常數
第一自旋角動量
U107
U104
U105
動量參數

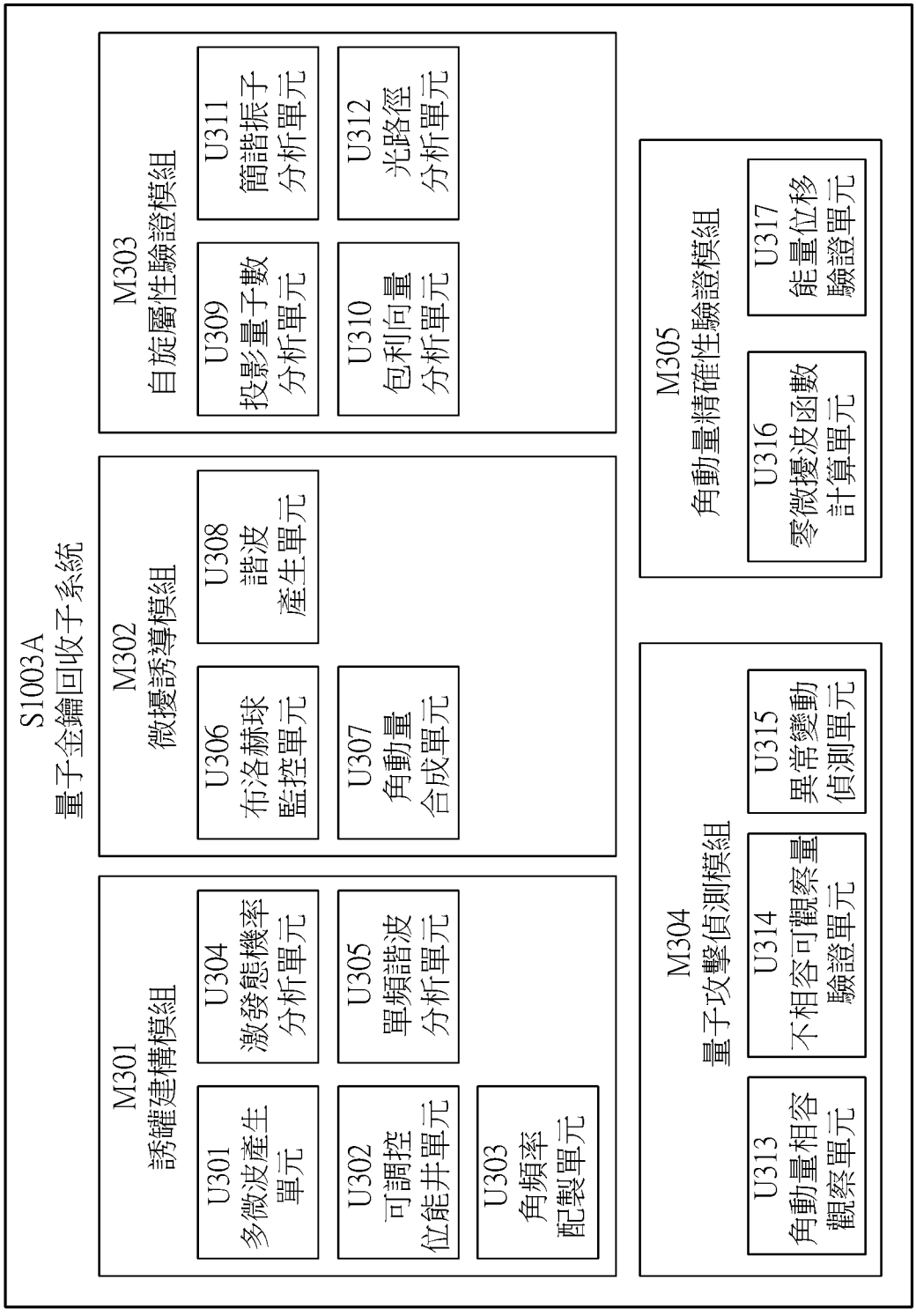
【圖3-2】


M1102
系統波函數分析模組
U101
量子系統量測單元
U10101
二次量子化
計算子單元
U10102
GW近似法
計算子單元
U10103
WKB近似法
計算子單元
U10104
變分近似法
計算子單元
U102
系統波函數分析單元
U10201
斯萊特行列式
計算子單元
U10202
包利矩陣
轉換子單元
U10203
玻恩定則
運算子單元
U10204
法蘭克-康登原理
分析子單元
U10205
絕熱近似
運算子單元

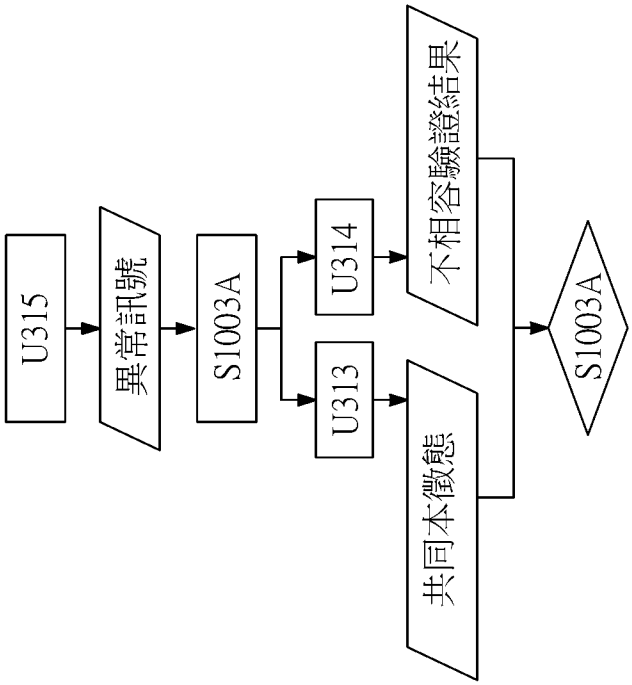
【圖4】


U10205
絕熱近似運算子單元
M10201
射影計算
子模組
M10202
福克空間
轉換子模組
M10203
希爾伯特
變換子模組
M10204
二次量子化
子模組
M10205
傅立葉轉換
子模組
M10206
泛函分析
子模組
M10207
歸一化運算
子模組
M10208
總均計算
子模組
M10209
薛丁格方程
轉換子模組

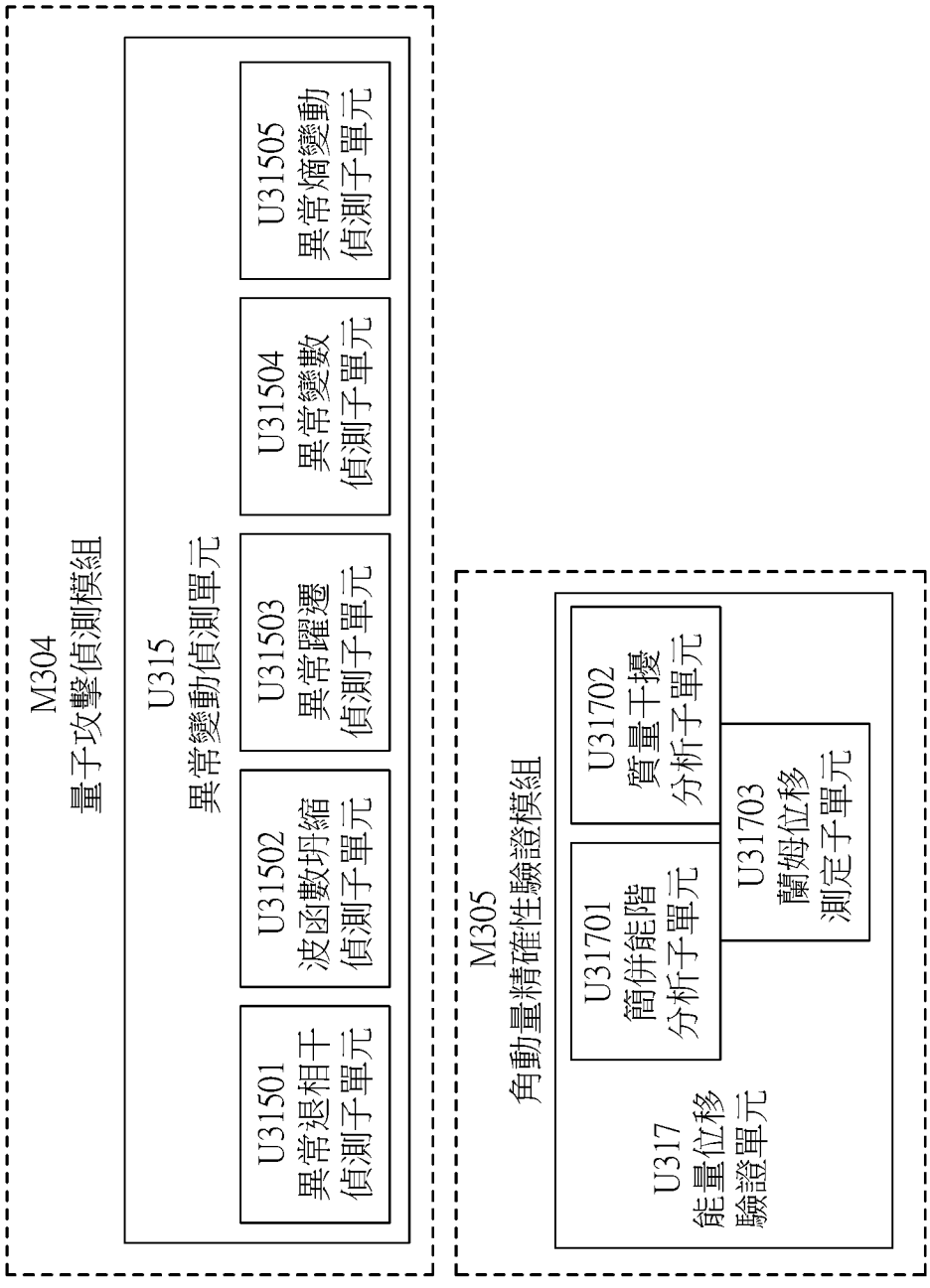
【圖5】


S1003A
量子金鑰回收子系統
M301
誘罐建構模組
U301
多微波產生單元
U302
可調控位能井單元
U303
角頻率配製單元
U304
激發態機率分析單元
U305
單頻諧波分析單元
M302
微擾誘導模組
U306
布洛赫球監控單元
U307
角動量合成單元
U308
諧波產生單元
M303
自旋屬性驗證模組
U309
投影量子數分析單元
U310
包利向量分析單元
U311
簡諧振子分析單元
U312
光路徑分析單元
M304
量子攻擊偵測模組
U313
角動量相容觀察單元
U314
不相容可觀察量驗證單元
U315
異常變動偵測單元
M305
角動量精確性驗證模組
U316
零微擾波函數計算單元
U317
能量位移驗證單元

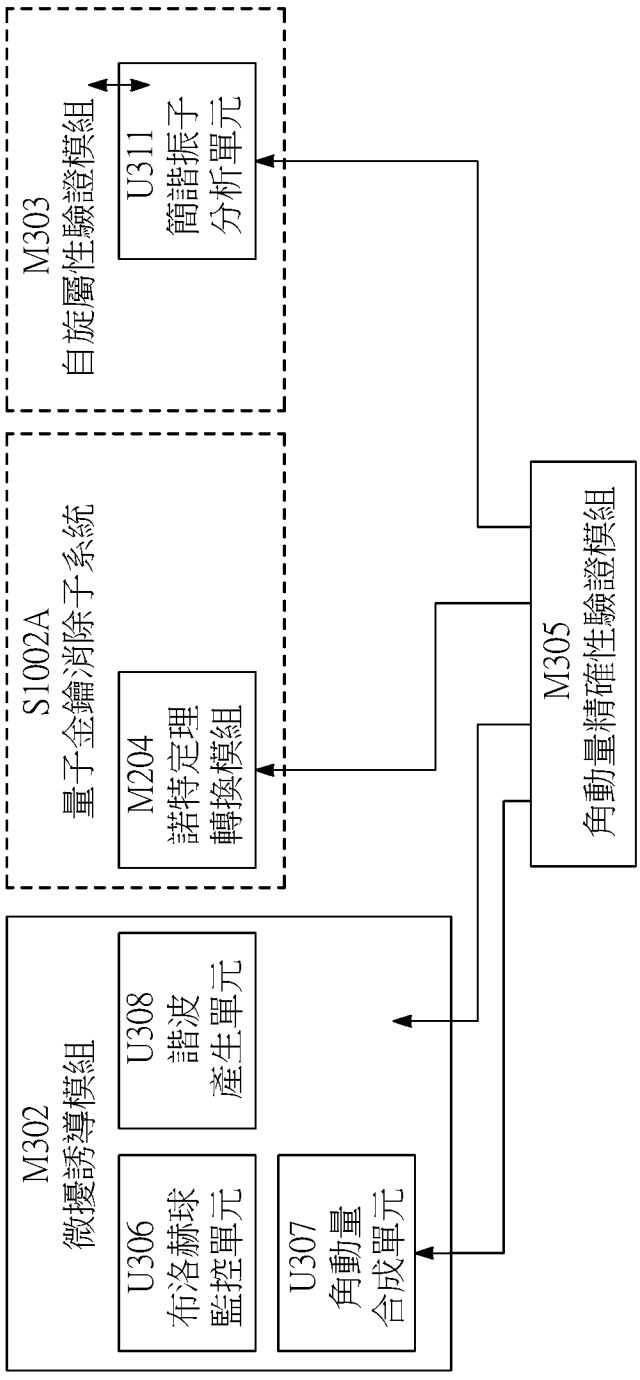
【圖6】



【圖7-1】


M304
量子攻擊偵測模組
U315
異常變動偵測單元
U31501
異常退相干
偵測子單元
U31502
波函數坍縮
偵測子單元
U31503
異常躍遷
偵測子單元
U31504
異常變數
偵測子單元
U31505
異常熵變動
偵測子單元
M305
角動量精確性驗證模組
U317
能量位移
驗證單元
U31701
簡併能階
分析子單元
U31702
質量干擾
分析子單元
U31703
蘭姆位移
測定子單元

【圖7-2】


M303
自旋屬性驗證模組
U311
簡諧振子
分析單元
S1002A
量子金鑰消除子系統
M204
諾特定理
轉換模組
M305
角動量精確性驗證模組
M302
微擾誘導模組
U308
諧波
產生單元
U306
布洛赫球
監控單元
U307
角動量
合成單元

【圖8】