公告本

發明專利說明書

580655

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：91123941　※IPC分類：G09C 1/00

※ 申請日期：91.10.17

壹、發明名稱

（中文）用於保護加密法則中計算之方法與裝置

（英文）METHOD AND APPARATUS FOR PROTECTING A CALCULATION IN A CRYPTOGRAPHIC ALGORITHM

貳、發明人（共 2 人）

發明人 1 （如發明人超過一人，請填**說明書發明人續頁**）

姓名：（中文）維南 費雪

（英文）WIELAND FISCHER

住居所地址：（中文）德國慕尼黑市慕勒街 11 號

（英文）MÜLLERSTRAβE 11, 80469 MUNICH, GERMANY

國籍：（中文）德國　（英文）GERMANY

參、申請人（共 1 人）

申請人 1 （如申請人超過一人，請填**說明書申請人續頁**）

姓名或名稱：（中文）德商億恒科技公司

（英文）INFINEON TECHNOLOGIES AG

住居所或營業所地址：（中文）德國慕尼黑市馬汀街 53 號

（英文）ST.-MARTIN-STRAβE 53, 81669 MUNICH, GERMANY

國籍：（中文）德國　（英文）GERMANY

代表人：（中文）1. 彼得 季里茲　2. 赫斯特 雪佛爾

（英文）1. PETER ZEDLITZ　2. HORST SCHAEFER

說明書發明人續頁

發明人 2

姓名：（中文）珍-皮爾 西弗

（英文）JEAN-PIERRE SEIFERT

住居所地址：（中文）德國慕尼黑市哈德弗街 1 號

（英文）HARSDOERFER STR. 1, 81669 MUNICH, GERMANY

國籍：（中文）德國 （英文）GERMANY

捌、聲明事項

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：＿＿＿＿＿＿＿＿＿＿

☑ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1.德國；2001 年 10 月 17 日；10151139.6

2.德國；2001 年 12 月 19 日；10162496.4

3.＿＿＿＿＿＿＿＿＿＿

☑ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號　順序註記】

1.德國；2001 年 10 月 17 日；10151139.6

2.德國；2001 年 12 月 19 日；10162496.4

3.＿＿＿＿＿＿＿＿＿＿

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號　順序註記】

1.＿＿＿＿＿＿＿＿＿＿

2.＿＿＿＿＿＿＿＿＿＿

3.＿＿＿＿＿＿＿＿＿＿

☐ 主張專利法第二十六條微生物：

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1.＿＿＿＿＿＿＿＿＿＿

2.＿＿＿＿＿＿＿＿＿＿

3.＿＿＿＿＿＿＿＿＿＿

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1.＿＿＿＿＿＿＿＿＿＿

2.＿＿＿＿＿＿＿＿＿＿

3.＿＿＿＿＿＿＿＿＿＿

☐熟習該項技術者易於獲得，不須寄存。

(1)

玖、發明說明

(發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明)

本發明係關於一種加密方式，明確地說，係關於一種用以保護一加密法則中計算之方法與裝置。

模指數係各種加密法則中其中一種非常重要的計算方式。舉例來說，其中一種廣泛運用的加密法則範例是由CRC Press於1996年出版，Menezes、van Oorschot、Vanstone共同著作的「Handbook of Applied Cryptography」第8.2章中所提到的RSA加密系統。RSA加密系統的作業方式如下。在該加密方式中，群B會對群A的一信息m進行加密。吾人假設，僅有群A可對接收自群B的加密信息進行解密。剛開始，群B會從群A接收公鑰。然後群B會以整數m表示欲進行加密的信息。接著，群B便會以下面的方式對信息m進行加密：

$$c = m^e \bmod n \qquad (1)$$

在方程式(1)中，m代表未加密的文字信息。e是公鑰。n是模數並且亦是公開的數字。c代表經過加密的信息。

現在，群B便會將經過加密的信息c傳送給群A。

為進行解密，也就是從秘密文字c中還原成未加密的文字m，必須執行下面的計算：

$$m = c^d \bmod n \qquad (2)$$

在方程式(2)中，d代表的是欲避免受到攻擊的群A的私鑰。

RSA簽章法則亦是本技藝中所熟知的。其包含下面的程序。每個實體A剛開始都會產生兩個很大的質數p及q，然後從p及q的乘積中計算出模數n。如上述專業書籍第11.3章中所述，可從中產生一密鑰，以便讓每一群都具有由n (也就

是模數)及e所組成的公鑰，而每一群則另外具有一私鑰d。

對RSA簽章的產生及驗證來說，實體A會對一信息m進行簽名。每個實體B都能夠驗證A'的簽章，並且從該簽章中擷取出信息m。

在該簽章的產生中，實體A剛開始會計算出一個整數m'＝R(m)。隨即，實體A便會進行下面的計算：

$$s = m'^{d} \bmod n \qquad (3)$$

其中s是A'對信息m所產生的簽章。

為驗證群A'的簽章，以及為擷取該信息m，群B必須進行下面的程序：

首先，群B必須從群A取得公鑰(n,e)。然後，群B便會進行下面的計算：

$$m' = s^{e} \bmod n \qquad (4)$$

在此方程式(4)之中，e是A'的公鑰。

接著，群B便會驗證m'是否為空間M_R中的元件。如果不是，便駁回該簽章。如果是，便可藉由計算$m = R^{-1}(m')$擷取出該信息m。

從上面的表示方法中，可清楚地看出，在眾多的場合中都會需要用到模指數。尤其是在方程式(2)的RSA加密，以及方程式(3)的RSA簽章產生中，都會使用私鑰d進行計算。

在典型的RSA系統中，因為私鑰的長度可能會非常的長(就如同公鑰般)，例如1024或2048個位元，所以模指數是一種非常龐大的計算方式，尤其是針對低功率的裝置(例如智慧卡、行動電話或PDA)來說更是如此。

為快速地計算該模指數，熟知的方式便是採用上面指定的專業書籍第2.120章中提及的所謂的中國餘數定理(CRT)。對RSA系統來說，特別適合使用葛納法則(Garner algorithm)(在上述的專業書籍第14.5.2章中亦有提及)。傳統的CRT法則一般都需要以模數M進行減模，不過，葛納法則則不需要。取而代之的是，後者的法則會將「大」模指數分成兩個「小」模指數，然後再根據中國餘數定理合併結果。即使此處需要兩個指數，不過，計算兩個「小」模指數仍然優於計算一個「大」模指數。

為表示使用葛納法則的RSA-CRT方法，可參考圖5。在方塊100中會設定輸入參數，其全都僅取決於p、q及密鑰d，但卻與欲進行簽章的信息m無關。在方塊102中，會如同以方程式(2)或方程式(3)的表示方式般，表示出該法則的輸出。應該注意的是，圖5所述的方法不僅適用於以私鑰所作的計算中，同時亦絕對可適用於使用公鑰的模指數運算中。

接著便會利用方塊100中所表示的輸入數值，於一方塊104中計算第一輔助模指數(sp)。同樣地，會在方塊106中計算第二輔助模指數(sq)。接著，便會在方塊108中根據中國餘數定理結合第一及第二輔助模指數的結果，產生$s = m^d \bmod n$的結果。一般來說，圖5所示的RSA-CRT方法會比利用平方及乘法法則直接計算方塊102所示的輸出快了大約四倍。

由於計算效率的關係，圖5中所示的RSA-CRT法則總是優於平方及乘法法則。不過，RSA-CRT法則的缺點是，非常容易受到加密「攻擊」，因為如果該RSA-CRT法則估算錯

誤時，亦或從中決定出密鑰d。Boneh、De-Millo、Lipton於第14期的J. Cryptology (2001)第101至119頁所發表的「On the Importance of Eliminating Errors in Cryptographic Computations」一文中，便敘述過此項問題。該份文件詳細地描述一種依照中國餘數定理(CRT)實現RSA的方法，其秘密簽章密鑰可能會由一單個錯誤的RSA簽章來決定。

因為執行法則的軟體或硬體發生錯誤都可能會產生錯誤的RSA簽章，舉例來說，將該加密處理器曝露在電氣或熱負載之中。

已經提出用以解決此類因硬體錯誤所引起的攻擊的對策是在從該晶片輸出之前都必須先驗證每個計算的輸出。即使此額外的驗證步驟可能會損及系統的效能表現，不過，為安全起見，此額外的驗證工作是不可或缺的。

最簡單的驗證方式便是利用公開的指數e進行逆計算，其目的是決定下面的等式：

$$(m^d)^e = m \bmod n \qquad (5)$$

不過，此額外的驗證工作就計算耗用直接與實際的簽章及/或解密步驟作比較之後，其僅能達到一半的系統效能表現，不過卻可提供極高的安全性。

不過，另一項優點則是一般的協定(例如ZKA-lib)無法使用該公鑰。ZKA-lib是一種管理可使用哪個資料的中央信用委員會(central credit committee)的規格總成。對該RSA-CRT方法來說，只有圖5方塊100中的輸入資料可以使用。此處，公鑰並非是ZKA-lib描述中的參數的一部份。所以，

必須利用大量的計算方能計算出指數e，以便依照等式(5)進行「逆計算」。如此一來可能會進一步地降低簽章晶片卡的效能，並且可能因為其慢速的作業模式，而無法趕上市場。

A. Shamir在Eurocrypt 97的Rump Session所發表的專業文章中「How to check modular Exponentiation」便敘述另一種方法，用以驗證由RSA-CRT方法所產生的簽章。此份專業文章建議使用小隨機亂數(例如，32位元)並且執行下面的計算取代方塊104中的計算：

$$sp' = m^d \bmod pr \qquad (6)$$

以下面的計算取代方塊106：

$$sp' = m^d \bmod qr \qquad (7)$$

在依照等式(6)及(7)進行計算之後，隨即進行下面的驗證計算：

$$sp' \bmod r = sq' \bmod r \qquad (8)$$

如果依照等式(8)的驗證結果正確時，便可從下面的等式(9)之中取得sp及sq：

$$sp' \bmod p = sp\ ;\ sq' \bmod q = sq \qquad (9)$$

接著，便可利用經由等式(9)所產生的sp及sq數值執行圖5方塊108中的計算，因此，便可利用中國餘數定理從輔助模指數中結合成整體的結果s。

此方法的缺點是僅驗證輔助參數r及中間結果sp'及sq'，如果所發生的一加密攻擊並未影響到中間結果sp'、sq'以及參數r，但是隨後卻造成一硬體錯誤時，此項驗證就不會禁止

輸出數值。舉例來說，在等式(9)及該法則最後進行結合的步驟中，便可能未經許可利用硬體錯誤探尋該密鑰d。

此外，在所引述的Boneh等人所發表的專業文章中建議，當處理器正在等待一外部的響應時，利用錯誤偵測位元保護一處理器的內部記憶體，以避開任何發生的暫存器錯誤，作為保護Fiat-Shamir技術的對策。另外的保護RSA簽章的方法則是造成該簽章方法的一隨機性。此隨機性可確保簽名器永遠不會對相同的信息簽名兩次。此外，如果驗證器呈現錯誤簽章時，其便無法知道所簽署的完整的未加密文字。

本發明的目的便係提供一種安全有效的概念，用以保護加密法則中的一計算。

藉由申請專利範圍第1項之方法或申請專利範圍第14項之裝置便可達成此項目的。

本發明係基於發現到輸入至一加密計算的資料(例如，圖5方塊100中的資料)最容易成為加密攻擊的「受害者」。經研究顯示，因為在一加密法則中作為計算的輸入資料最容易遭受惡意攻擊的影響，同時其對加密計算結果的影響程度並不會相同，所以能夠偵測到該些加密攻擊。吾人發現到輸入資料即加密攻擊的指示符號。如果經過加密法則中的計算之後，輸入資料與其在一加密法則之前的狀態比較之後並未改變時，便可安全地假設未發生任何加密攻擊。然而，如果經過加密法則中的計算之後，輸入資料與其原始狀態比較之後發生改變時，便可安全地假設已經發生一

加密攻擊。

所以，在本發明用以保護加密法則中計算的方法中，剛開始會提供輸入資料供加密計算使用。隨即，便會進行計算取得該計算的輸出資料。當執行該項計算之後，便會驗證該輸入資料在計算期間是否改變，為使其能夠精確，必須使用不同於該項計算本身的驗證法則。如果驗證結果證實，該輸入資料已經在計算期間被改變，便會禁止轉送該計算的輸出資料。

本發明的其中一項優點是，本發明的概念可省略中間結果，也就是，該項計算的輸出資料。因為，輸入資料便是一個安全的指示符號，可用以表示是否發生攻擊。根據本發明，在轉送該計算的任何輸出資料進行輸出或轉送給後續的計算之前，會先進行驗證該輸入資料在計算期間是否改變。因此，輸入資料便可當作一加密攻擊的「感測器」。

本發明的其中一項優點是，可採用比加密計算本身便宜甚多的驗證法則，因此便可節省該具有公開指數的「逆計算」所需要的費用。

本發明的另一項優點是，與熟知的概念(其中需要輔助指數的輸出資料進行驗證)比較起來，可更安全地偵測到加密攻擊。需要計算的中間結果的概念一般都僅能夠判斷在中間結果的計算期間是否發生錯誤，即該處理器的內部計算單元是否因錯誤攻擊而無法正常地作業。

不過，如果該加密攻擊相當「薄弱」，僅影響該記憶體而不會影響該計算單元時，根據中間結果的驗證方法便能

辨別出此項錯誤。然而，一但該計算單元於日後存取有缺陷的記憶體以輸詢一後續計算的參數時，將會發生錯誤，而讓攻擊者得逞。舉例來說，當方塊108中的計算單元存取記憶體以輸詢qinv、p或q時，便會發生此種存取作業。熟知的保護方法並無法捕捉到此種錯誤。

當進行加密計算之後，可使用各種可能方式驗證該輸入資料。其中一種可能方式是在儲存該輸入資料時形成一檢查和，並且儲存該檢查和。當進行加密計算之後，可存取相同的記憶體位置擷取出其內容，並且利用應該具有輸入資料的記憶體位置內容形成一檢查和。如果該檢查和與所儲存的檢查和相同時，便可輸出該項計算的結果。如果依照輸入資料的記憶體內容所形成的檢查和與儲存在記憶體中的檢查和不相同時，便可假設已經發生加密攻擊，此即何以無任何資料輸出，而僅有錯誤信息或是完全沒有任何信息的原因。

另一種驗證輸入資料的較佳替代例則是，在將輸入資料儲存至晶片卡本身的期間，或在開始進行計算時，利用處理法則處理該輸入資料，以便決定可儲存於安全資訊記憶體位置中的安全資訊。當執行加密法則之後，便可擷取出該安全資訊記憶體位置的內容，並且根據檢查法則進行處理。該檢查法則可設計成，如果該安全資訊記憶體位置的內容未被改變時，便會得到預設的結果。如果得到此結果時，便可假設未發生攻擊。不過，如果未得到此結果時，便很可能發生攻擊，所以必須禁止該加密法則的計算輸出

資料。

舉例來說，其中一種適當的處理法則是將數字乘以一個整數。與此處理法則對應的檢查法則是對具有原始數字的安全資訊進行減模。那麼，便可將「0」視為預設的結果。當然，亦可考慮另外的檢查法則，其特徵同樣是在對從輸入資料推衍出來的安全資訊進行處理之後(更明確地說，在進行該項計算之前)提供一預設的結果。

下文中將參考圖式來詳細說明本發明較佳具體實施例，其中：

圖1所示的係本發明概念的一方塊圖；

圖2a及2b所示的係根據本發明一第一具體實施例之具有一檢查和法則的本發明概念之一較詳細示意圖；

圖3a及3b所示的係使用本發明第二具體實施例之本發明概念之一較詳細示意圖；

圖4所示的係使用RSA-CRT方法之本發明概念之一詳細示意圖；以及

圖5所示的係熟知的RSA-CRT方法一方塊圖。

用以保護一加密法則中一計算之本發明裝置中，剛開始其包括一裝置10，用以提供加密法則(舉例來說，用以進行加密/解密或簽章/驗證的RSA法則)之一部份的計算的輸入資料。該提供裝置10會供應計算的輸入資料，該輸入資料會被饋送至裝置12，用以進行加密計算，或是進行一加密法則的計算。裝置12會供應該計算的輸出資料。為安全起見，現在並不會單純地輸出或供應該計算的輸出資料進行

進一步的計算，例如，而是不論是否發生加密攻擊，都會將其延後一段時間，直到裝置14驗證輸入資料中的一變化。

裝置14會利用該輸入資料執行該項驗證。如果與執行加密計算之後比較起來，執行加密計算之前的輸入資料狀態沒有產生任何變化時，便可假設並未發生任何攻擊，因此，便可將裝置12輸出處的輸出資料輸出至顯示器，或是供應作為進一步計算的輸入資料。不過，如果裝置14發現該輸入資料已經被改變時，便會啟動裝置16禁止該輸出資料。視實現的方式而定，除了禁止該輸出資料之外，亦可輸出錯誤信息。或者，完全不產生輸出。

圖2a及2b所示的係根據檢查和法則之本發明第一具體實施例之詳細示意圖。在方塊20中，剛開始會將加密法則之計算(例如，圖5所示的RSA-CRT計算)的輸入資料儲存在加密處理器的輸入資料記憶體位置中。接著，在首次將該資料儲存於該卡片上的期間，便會在該輸入資料中形成一檢查和(例如CRT檢查和)，因而便可將該檢查和儲存在該加密處理器的檢查和記憶體位置中(方塊22)。

如圖2b所示，圖1的裝置14可設計成於計算該加密法則之後存取該輸入資料記憶體位置，以便擷取出該輸入資料記憶體位置的內容(方塊24)。如一方塊26所示，接著便可使用如方塊22般相同的法則，在所擷取的輸入資料記憶體位置的內容中形成一檢查和。在方塊26的輸出處便會產生目前所計算的輸入資料檢查和。隨後，便可藉由方塊28存取方塊22儲存在檢查和記憶體位置處的檢查和(圖2a)。最後，在

方塊30會比較所儲存的檢查和以及目前所計算的檢查和(由方塊26所計算的)。如果有任何差異時，便可假設輸入資料已經在執行該加密法則計算期間遭到破壞，此即代表有錯誤攻擊。所以，必須禁止該輸出資料。如果該些檢查和沒有任何差異時，便可假設未發生任何攻擊，因此可輸出該輸出資料，或是將其傳輸作為一進一步加密計算的輸入資料。

下面將參考圖3a及3b敘述驗證加密法則之計算的輸入資料中的變化的替代具體實施例。如圖2a所示的具體實施例般，剛開始會將輸入資料儲存在輸入資料記憶體位置中(方塊32)。與圖2a所示的具體實施例(其中會計算出檢查和)不同的是，現在會利用一處理法則處理該輸入資料，以便得到安全資訊(方塊34)。接著，一方塊36便會將方塊34所計算的安全資訊儲存在該加密處理器的安全資訊記憶體位置中。

現在會以下面的方式進行驗證。如圖3b的方塊38所示，剛開始會擷取出位於該安全資訊記憶體位置中的資訊。然後，在一方塊40中利用檢查法則處理此資訊，該檢查法則的實現方式可在該安全資訊記憶體位置中的內容未發生變化時提供一預設的結果。在方塊42中，會驗證經過方塊40中的檢查法則處理之後，是否產生預設的結果。如果是時，便會如同方塊44所示般地轉送該輸出資料。不過，如果發現經過檢查法則40處理之後並未產生預設的結果時，便會禁止該輸出資料(方塊16)。

下面將參考圖4說明用以安全地執行RSA-CRT方法的較佳

具體實施例，其中，可在該法則內不同的地方採用本發明的概念，用以在輸出加密法則之輸出資料之前先驗證該輸入資料。

此外，在圖4所示的具體實施例中亦會驗證該加密法則的計算本身，尤其是該兩個輔助指數的計算。最後，在圖4所示的具體實施例中，亦會驗證該兩個輔助指數的結果是否已正確的方式進行「結合」，用以取得已經簽章的信息s。

如圖5所示，剛開始會提供參數p、q、dp、dq、qinv，該些參數都是RSA-CRT方法經常使用的輸入參數。如圖4的方塊50所示，會進一步提供欲加密的信息m、數值t以及隨機亂數rand。數值t較佳的係一質數，而且較佳的係不超過16位元的小質數，以免對該CRT方法(也就是，與利用模數n＝p×q的單模指數運算比較起來，其係利用小模數執行兩個輔助指數)的優點影響太多。當然，數值t亦可能不是質數，不過，必須以t的Euler Phi函數取代該些等式中的運算式(t−1)。

如圖4所示，剛開始會在方塊52a、52b中處理輸入資料。將原來的參數p及/或q乘以質數t之後便可作為該處理法則。接著，便會將dp與隨機亂數rand及數值(p−1)的乘積相加，作為該處理規格，對q來說亦可進行相同處理。

應該強調的是，原則上，方塊52a、52b的四項處理規格中任一項都可達到本發明的效果。完成方塊52a、52b之後，便會將該項處理所取得的安全資訊p'、dp'、q'及dq'儲存在安全資訊記憶體位置中。舉例來說，此記憶體位置可能是

加密處理器的工作記憶體，或是與該加密處理器計算單元相關的內部暫存器。隨即，如方塊54a、54b所示，該計算單元會計算第一輔助指數(sp')及第二輔助指數(sq')，作為該加密法則內的計算，如圖4所示。在執行方塊54a、54b之後，該些計算的輸出資料(即sp'與sq')並不會直接輸出及/或不會直接轉送給進一步的計算使用，而是會根據本發明驗證(利用檢查法則於方塊56a、56b開始進行)在該項計算期間，方塊54a、54b之計算的輸入資料是否被方塊54a、54b改變。為達此目的，會使用減模作為檢查法則，其中，如方塊56a、56b的第一行所示，可將0視為預設的結果，或是將dp或dq視為預設的結果。如果變數p'(在本發明中，其為安全資訊)並未因為錯誤攻擊而改變時，便會產生預設的結果。同樣的原理亦適用於另一安全資訊dp'。

如果方塊56a、56b中經由檢查法則驗證的結果成功時，即得到預設的結果，該過程便會進輸入資料方塊58a、58b。方塊58a、58b顯示的係較佳的前置計算，不但可執行輸入資料驗證概念，亦可執行結果資料驗證概念。接著，便可透過結果檢查法則(圖4中的方塊60)驗證方塊54a、54b中的輔助指數運算是否正確。

在方塊62a、62b中，方塊54a、54b中的輔助指數會經過對應的減模處理，以減少參數t及/或隨機亂數的影響。從圖5的方塊108中便可非常地清楚，最後會在方塊64中進行結合步驟，以便從該些輔助指數的結果sp、sq中產生經過簽章的信息s。

不過，在本發明之較佳具體實施例中，並不會直接使用此結果，而是會驗證經過方塊64的結合之後，其結合結果是否成功。

欲達到此目的，可利用質數p作為模數，對所取得的已簽章的信s進行減模處理。此檢查法則應該會以sp作為輸出結果，此sp必須等於方塊62a中所計算的數值sp。

在方塊66b中則會進行類似的方式，同樣利用質數q作為模數，以減模處理驗證結果s的正確度。為達此目的，剛開始會存取儲存著方塊64之結果的中間記憶體位置，以便執行方塊66a中的計算。此外，還會存取儲存著輸入資料p的記憶體位置。最後，會存取儲存著方塊62a之結果(即sp)的記憶體位置，以便執行方塊66a中的比較。在方塊66b中則會對s、q及sq進行類似的程序。

如果方塊66a中的計算產生預設的結果，使得方塊66a中等式的左邊及右邊並不相同時，便會輸出錯誤，並且禁止輸出方塊64的結果。如果方塊66b中的計算亦發現有錯誤發生時，同樣會禁止結果s。因此，較佳的係，如果某個方塊產生錯誤時，便加以禁止，或是，換句話說，只有當方塊66a中的計算及方塊66b中的計算都正確的時候才會利用方塊68輸出結果。

在方塊66a中相當明顯的是，此結果檢查法則的優點是，其直接使用方塊64的結果進行驗證，不過，其亦會存取輸入資料記憶體區以便取得質數p及/或p的位置所在處的記憶體位置的內容，並且還會額外地使用於步驟62a中所取得的

中間結果，即sp。因此，會經由計算以驗證是否有任何的輸入資料發生變化，以及驗證該加密運算單元是否正確地執行RSA-CRT方法的結合步驟64。最後，亦會使用中間結果sp，因此中間結果暫存器亦必須內含於單個簡單的計算中。

從圖4所示的具體實施例中可清楚地看出，用以產生該安全資訊的處理法則，以及用以驗證該輸入資料的檢查法則都是該加密運算單元中的簡單法則，例如乘法法則或用以進行減模的法則。對於方塊62a、62b (其同樣是根據減模運算)中的處理法則以及方塊66a、66b (其亦是根據減模運算)中的檢查法則同樣適用。

雖然在圖4所示的前述具體實施例中，利用數值與常數的乘法作為處理法則，並且利用原來的數值對該乘法結果進行減模運算作為對應此處理法則的檢查法則，不過，熟習本技藝的人士非常地清楚處理法則與檢查法則的數值會彼此對應，所以能夠驗證在進行加密法則的計算中，輸入資料是否因為錯誤攻擊而發生變化。

此外，從圖4中可清楚地看出，如同檢查法則般，可以非常簡單的方塊式來實現該處理法則，並且除了所述的參數之外並不需要額外的參數。明確地說，根據本發明，較佳的係不需要以非常昂貴的方式計算任何額外的參數，例如公鑰e，然後再用以進行「逆計算」，取而代之的是儘可能相互連結非常多的輸入資料、中間結果資料等，因為藉此便可利用單一的驗證步驟偵測到該工作記憶體、該內部暫

存器或該運算單元本身之中可能會發生的錯誤，以便在發生錯誤時禁止資料輸出，所以，絕對不會從不正確的輸出中決定秘密資訊。

圖式代表符號說明

10 提供輸入資料的裝置

12 執行一加密計算的裝置

14 驗證輸入資料中的一變化的裝置

16 禁止輸出資料的裝置

20 將該輸入資料儲存在輸入資料記憶體位置

22 形成且儲存一檢查和

24 從該輸入資料記憶體位置進行擷取

26 在該輸入資料記憶體位置的內容中形成一檢查和

28 擷取該檢查和記憶體位置的內容

30 比較該些檢查和

32 將該輸入資料儲存在輸入資料記憶體位置

34 處理該輸入資料以便取得安全資訊

36 將該安全資訊儲存在安全資訊記憶體位置

38 擷取該安全資訊儲存位置的內容

40 利用一檢查法則進行處理

42 就預設結果加以驗證

44 轉送該輸出資料

50 RSA-CRT法則的輸入資料

52a，52b 處理該輸入資料以便取得安全資訊

54a，54b 計算該加密法則

56a，56b 利用一檢查法則處理該安全資訊，並且驗證是否得到一預設結果

58a，58b 產生檢查法則

60 利用檢查法則進行驗證

62a，62b 簡化sp'及/或sq'

64 結合法則

66a，66b 驗證法則的第一部份及第二部份

68 輸出數位簽章S

100 RSA-CRT方法的輸入資料

102 RSA-CRT方法的輸出資料

104 計算一第一輔助指數

106 計算一第二輔助指數

108 結合第一及第二輔助指數

肆、中文發明摘要

在用以保護一加密法則中一計算之方法中，該計算會取得輸入資料以產生輸出資料，一開始即提供該計算的輸入資料(10)。隨即，便會執行該項計算(12)以取得該計算的輸出資料。當執行計算之後，便會驗證(14)該輸入資料在計算期間是否改變，更明確地說，必須使用不同於該項計算本身的驗證法則。如果驗證結果證實該輸入資料已經在計算期間被改變，便會禁止轉送該輸出資料(16)。由於輸入資料特別容易遭受到硬體攻擊，藉此方式便可非常確定不會輸出不正確的加密法則計算結果。此外，與計算該加密法則本身比較起來，僅需要稍微觀察其完整性便可檢查該輸入資料。

伍、英文發明摘要

In a method for protecting a calculation in a cryptographic algorithm, the calculation obtaining input data so as to create output data, input data for the calculation are initially provided (10). Subsequently, the calculation is performed (12) so as to obtain the output data of the calculation. After the calculation has been performed, a verification is carried out (14) as to whether the input data was changed during the calculation, to be precise using a verification algorithm which differs from the calculation itself. If the verification proves that the input data was changed during the calculation, forwarding of the output data is suppressed (16). By doing so, outputting of incorrect results of the calculation of the cryptographic algorithm is prevented with a high degree of certainty, since the input data is particularly susceptible to hardware attacks. In addition, the input data may be examined with a view to their integrity with little expenditure compare to calculating the cryptographic algorithm itself.

陸、(一)、本案指定代表圖為：第 1 圖

(二)、本代表圖之元件代表符號簡單說明：

10　提供輸入資料的裝置

12　執行一加密計算的裝置

14　驗證輸入資料中的一變化的裝置

16　禁止輸出資料的裝置

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

拾、申請專利範圍

1.一種用以保護一加密法則中一計算之方法，該計算會取得輸入資料以產生輸出資料，該方法包括：

提供(10)該輸入資料以進行計算；

執行(12)該計算以取得該計算的輸出資料；

當執行該項計算之後，使用不同於該項計算的一驗證法則驗證(14)該輸入資料在計算期間是否改變；以及

如果該驗證(14)證實該輸入資料已經在計算期間被改變，便會禁止(16)轉送該計算的輸出資料。

2.如申請專利範圍第1項之方法，其中在提供該輸入資料的該步驟中，該輸入資料係儲存在一輸入資料記憶體位置(20)；

其中在該輸入資料的至少一部份中形成一檢查和並且儲存在一檢查和記憶體位置中(22)；以及

其中該驗證法則包括下面的子步驟：

擷取(24)該輸入資料記憶體位置的內容；

在所擷取的內容之至少一部份中形成(26)一檢查和；

擷取(28)該檢查和記憶體位置的內容；以及

比較(30)由所擷取的檢查和記憶體位置的內容所構成的檢查和；以及

其中如果比較結果出現一差異時，便禁止(16)轉送該輸出資料。

3.如申請專利範圍第1項之方法，

其中在該提供步驟中，該輸入資料會儲存在一輸入資料記憶體位置中(32)；

其中會根據處理法則處理該輸入資料的至少一部份(34)以便取得安全資訊，並且將該安全資訊儲存在一安全資訊記憶體位置中(36)；

其中該驗證法則包括：

擷取(38)該安全資訊記憶體位置的內容的至少一部份；

利用一檢查法則處理(40)該安全資訊記憶體位置的內容，該檢查法則的設計方式可在該安全資訊記憶體位置中的內容未發生變化時提供一預設的結果(42)；以及

其中，如果該檢查法則所提供的一結果與預設結果不同時，便禁止(16)轉送該輸出資料。

4.如申請專利範圍第1項之方法，

其中該加密法則包括一進一步的計算；以及

其中若該驗證法則提供預設結果時，該安全資訊便可作為進一步計算的輸入資料。

5.如申請專利範圍第3項之方法，

其中該驗證法則進一步包括擷取該輸入資料記憶體位置的一步驟，以便擷取該輸入資料記憶體位置的內容的至少一部份；以及

其中該檢查法則係配置以進一步使用該輸入資料記憶體位置的內容的至少一部份。

6.如申請專利範圍第3項之方法，

其中用以產生該安全資訊的處理法則包括將代表輸入資

料一部份的一輸入數值與一整數相乘；

其中該檢查法則包括以該輸入數值當作模數對該安全資訊的記憶體位置的內容進行一減模運算；以及

其中該預設的結果為「0」。

7.如申請專利範圍第3項之方法，其中該處理法則包括將一第一輸入數值以及一隨機亂數與小於1的一第二輸入數值乘積相加密法則：

其中該檢查法則包括以該小於1的第二輸入數值當作模數對該安全資訊的記憶體位置的內容進行一減模運算；

其中該預設的結果為該第一輸入數值。

8.如申請專利範圍第1項之方法，其中該加密法則係利用中國餘數定理(CRT)所進行的RSA法則之模指數運算。

9.如申請專利範圍第8項之方法，其中m、p、q、dp、dq、qinv、t及rand都是輸入資料，其中m是一欲處理的未加密文字信息，其中p及q代表的是第一及第二質數，其乘積等於一模數n，其中dp是一第一輔助指數，其中dq是一第二輔助指數，其中qinv等於$q^{-1} \bmod p$，其中t是一質數，以及其中rand是一隨機亂數。

10.如申請專利範圍第9項之方法，其中該處理法則可以下面的方式來實現：

$p' = p \cdot t$；

$dp' = dp + rand \cdot (p-1)$；

$q' = q \cdot t$；及/或

$dq' = dq + rand \cdot (q-1)$，以及

其中該檢查法則可以下面的方式來實現：

$p' \bmod p = 0$；

$q' \bmod q = 0$；

$dp' \bmod (p-1) = dp$；及/或

$dq' \bmod (q-1) = dq$；以及

其中該加密計算如下：

$sp' = m^{dp'} \bmod p'$；或

$sq' = m^{dq'} \bmod q'$；

其中，p'、q'、dp'、dq'都是安全資訊，其中dp、dq及0都是預設的結果，以及

其中，sp'、sq'都是該加密法則計算的輸出資料。

11.如申請專利範圍第1項之方法，進一步包括：

利用該加密法則的一計算結果及該輸入資料記憶體位置的內容執行結果檢查法則，該結果檢查法則與該項計算不同，而且如果該輸入資料記憶體位置包含未改變的內容而且正確地執行該加密計算時可提供一預設結果；以及

如果該檢查法則所提供的一結果與預設結果不同時，便禁止轉送。

12.如申請專利範圍第11項之方法，其中該計算如下：

$sp' = m^{dp'} \bmod p'$；及/或

$sq' = m^{dp'} \bmod q'$；

其中，該結果檢查法則如下：

$spt = sp' \bmod t$；

$sqt = sq' \bmod t$；

$dpt = dp' \bmod (t-1)$；

$dqt = dq' \bmod (t-1)$；

$spt^{dqt} = sqt^{dpt} \bmod t$；以及

其中，該預設的結果為一等式。

13.如申請專利範圍第11項之方法，其中該加密法則包括利用中國餘數定理(CRT)所進行的RSA法則之一模指數運算，其中該計算如下：

$s = sq + \{[(sp-sq) \cdot qinv] \bmod p\} \cdot q$；及

其中，該結果檢查法則如下：

$s \bmod p = sp$；及/或

$s \bmod q = sq$，

其中該預設的結果為一等式條件。

14.一種用以保護一加密法則中一計算之裝置，該計算會取得輸入資料以產生輸出資料，該裝置包括：

一用以提供(10)輸入資料進行計算之裝置；

一用以執行(12)該項計算以取得該計算的輸出資料之裝置；

一用以利用一不同於該項計算的驗證法則驗證(14)該輸入資料在計算期間是否改變之裝置，該驗證裝置係設計成在執行該項計算之後才進行驗證；以及

一裝置，如果該驗證裝置(14)判斷出該輸入資料已經在計算期間被改變，該裝置便可禁止(16)轉送任何的輸出資料。

拾壹、圖式

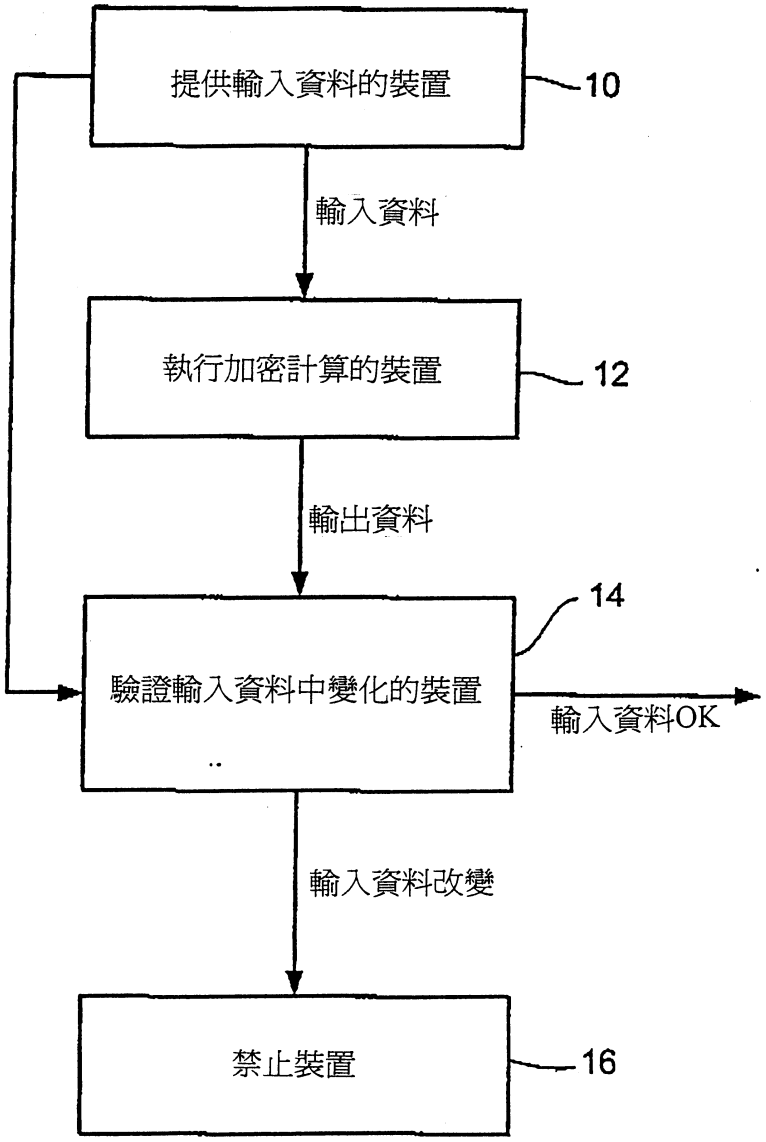
提供輸入資料的裝置
10
輸入資料
執行加密計算的裝置
12
輸出資料
14
驗證輸入資料中變化的裝置
輸入資料OK
輸入資料改變
禁止裝置
16

圖1

圖式續頁

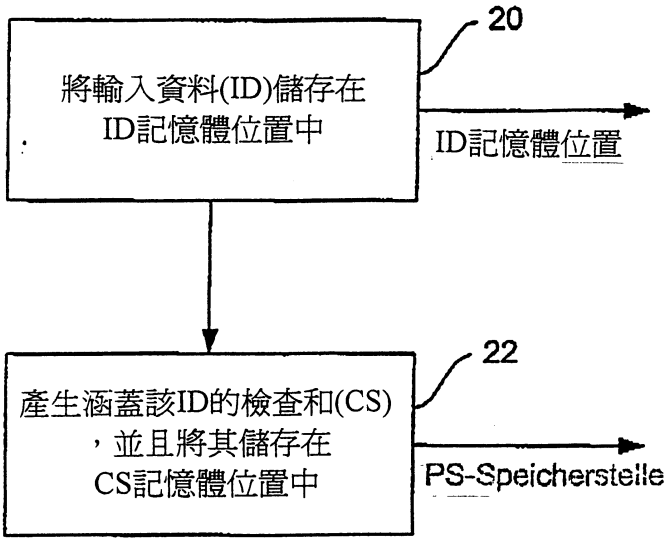
20
將輸入資料(ID)儲存在
ID記憶體位置中
ID記憶體位置
22
產生涵蓋該ID的檢查和(CS)
，並且將其儲存在
CS記憶體位置中
PS-Speicherstelle

圖2a

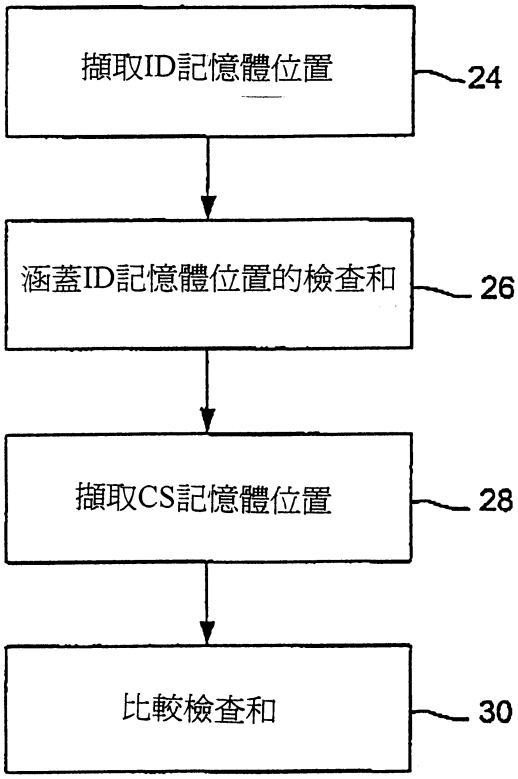
擷取ID記憶體位置
24
涵蓋ID記憶體位置的檢查和
26
擷取CS記憶體位置
28
比較檢查和
30

圖2b

圖式續頁

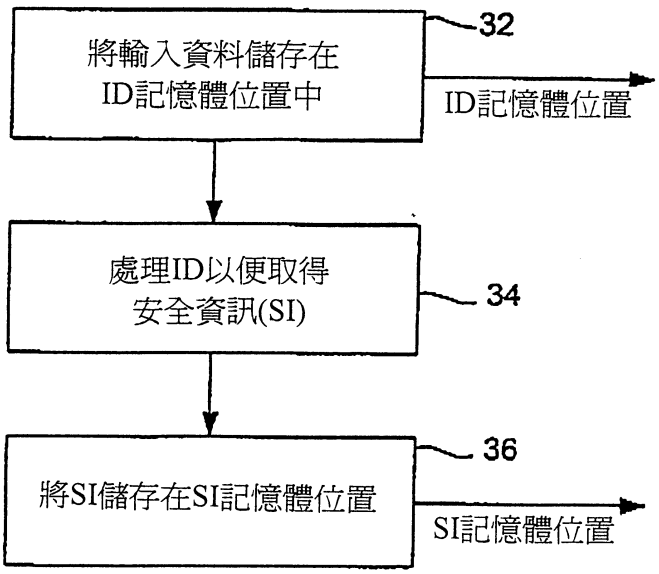
將輸入資料儲存在
ID記憶體位置中
32
ID記憶體位置
處理ID以便取得
安全資訊(SI)
34
將SI儲存在SI記憶體位置
36
SI記憶體位置

圖3a

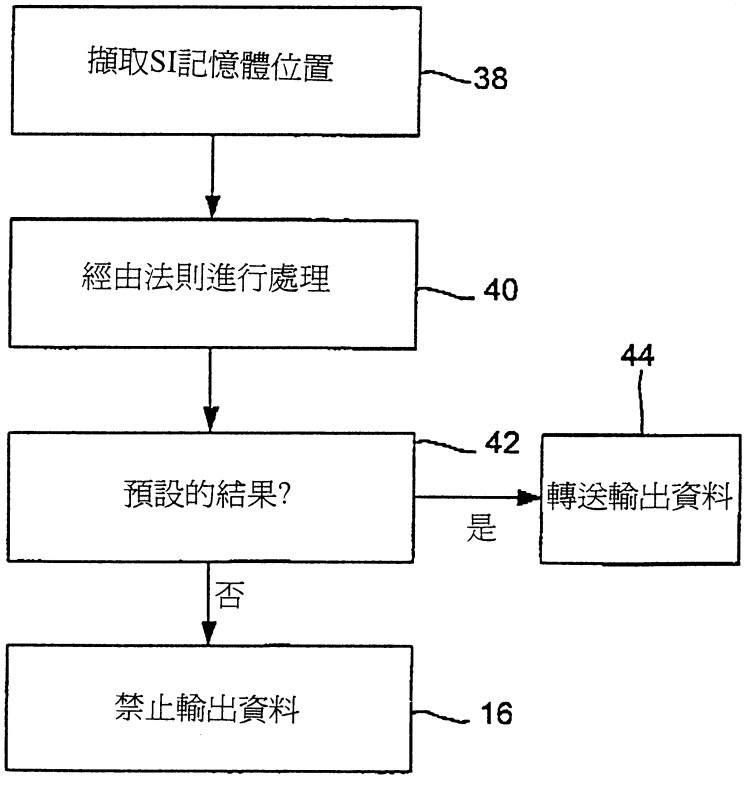
擷取SI記憶體位置
38
經由法則進行處理
40
44
預設的結果?
42
轉送輸出資料
是
否
禁止輸出資料
16

圖3b

圖式續頁

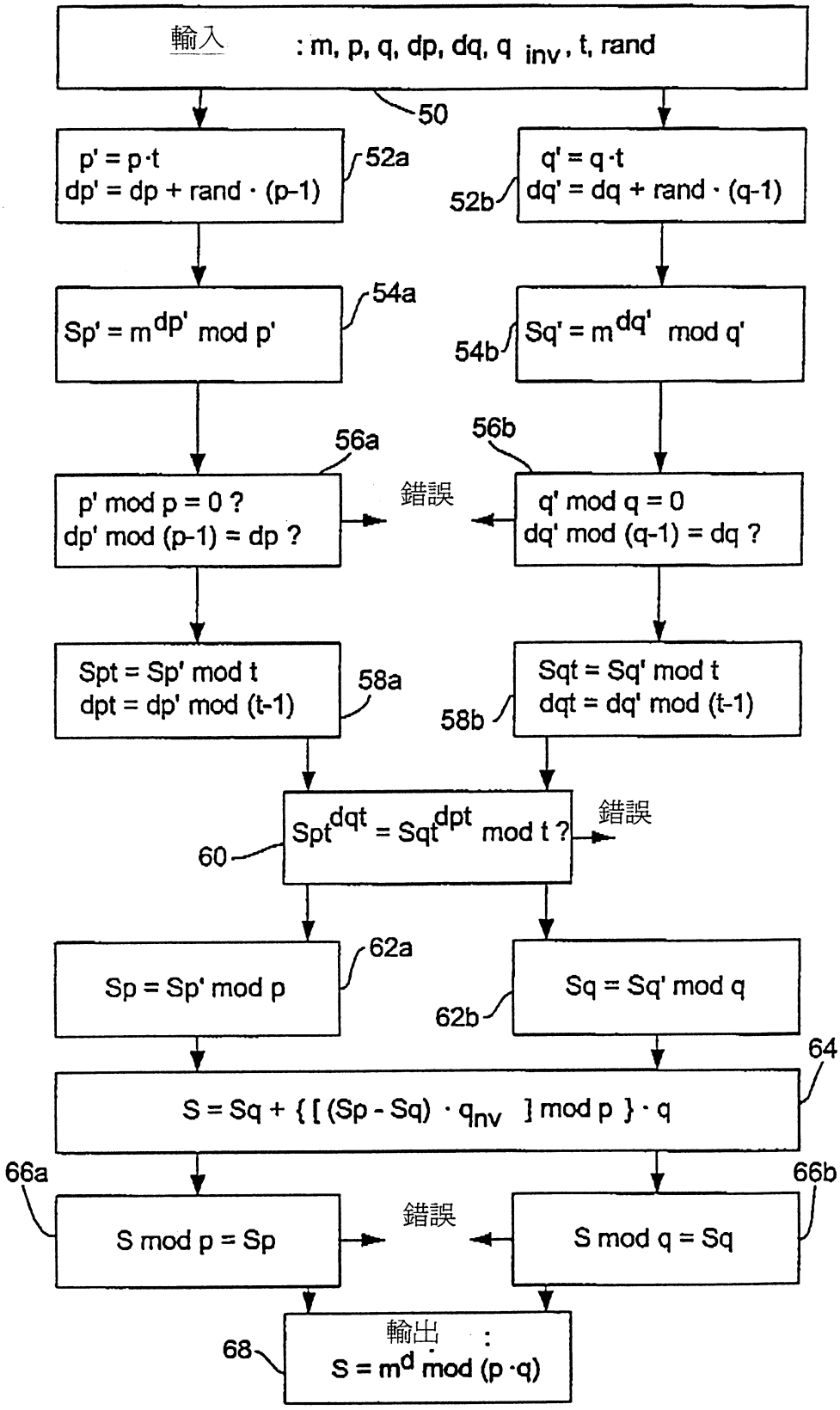
輸入 : m, p, q, dp, dq, q inv, t, rand
50
p' = p·t
dp' = dp + rand · (p-1)
52a
q' = q·t
dq' = dq + rand · (q-1)
52b
Sp' = m^dp' mod p'
54a
Sq' = m^dq' mod q'
54b
56a
56b
p' mod p = 0 ?
dp' mod (p-1) = dp ?
錯誤
q' mod q = 0
dq' mod (q-1) = dq ?
Spt = Sp' mod t
dpt = dp' mod (t-1)
58a
Sqt = Sq' mod t
dqt = dq' mod (t-1)
58b
Spt^dqt = Sqt^dpt mod t ?
60
錯誤
Sp = Sp' mod p
62a
Sq = Sq' mod q
62b
64
S = Sq + { [(Sp - Sq) · q inv] mod p } · q
66a
66b
S mod p = Sp
錯誤
S mod q = Sq
輸出 :
S = m^d mod (p·q)
68

圖4

圖式續頁

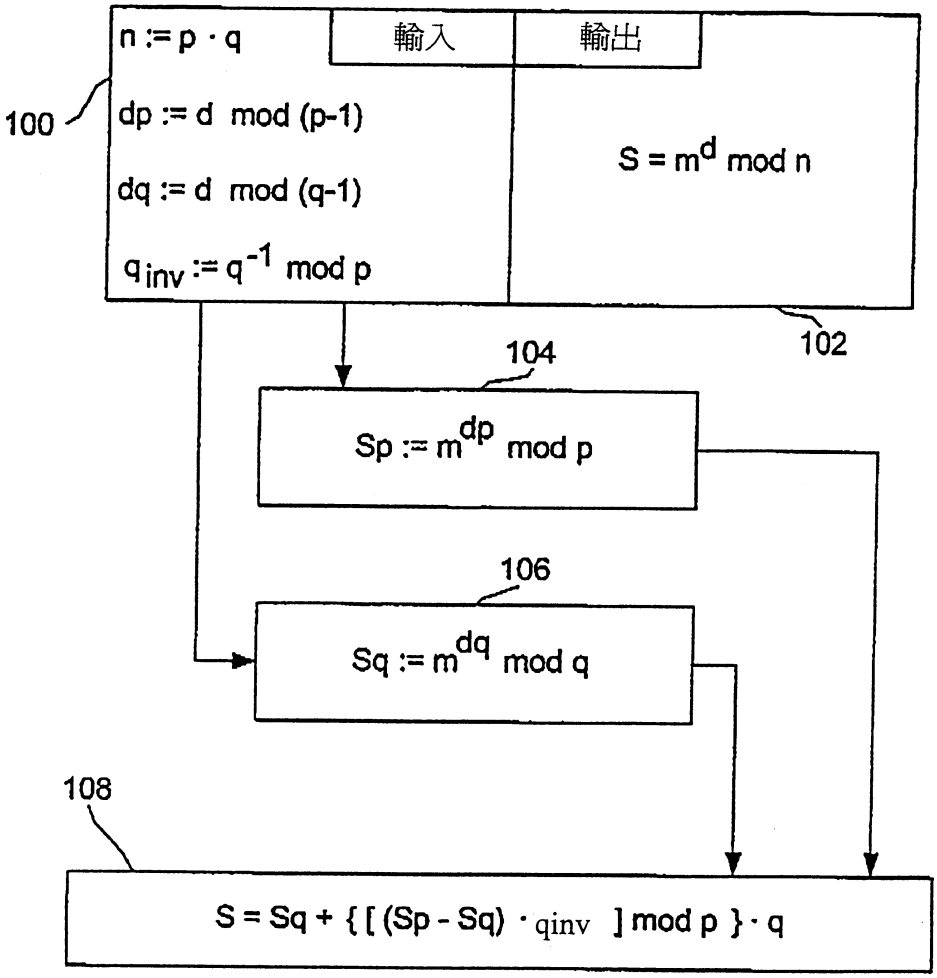
n := p · q
輸入
輸出
100
dp := d mod (p-1)
dq := d mod (q-1)
$q_{inv} := q^{-1} \bmod p$
$S = m^d \bmod n$
102
104
$Sp := m^{dp} \bmod p$
106
$Sq := m^{dq} \bmod q$
108
$S = Sq + \{ [(Sp - Sq) \cdot qinv] \bmod p \} \cdot q$

圖5

(先前技藝)