(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 201225613 A1
(43)公開日： 中華民國 101 (2012) 年 06 月 16 日

(21)申請案號：099144013 (22)申請日： 中華民國 99 (2010) 年 12 月 15 日
(51)Int. Cl.： *H04L9/00 (2006.01)*
(71)申請人：國立交通大學 (中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)
新竹市大學路 1001 號
(72)發明人：劉柏均 LIU, POCHUN (TW) ；張錫嘉 CHANG, HSIECHIA (TW) ；李鎮宜 LEE, CHENYI (TW)
(74)代理人：蔡坤財；李世章
申請實體審查：有 申請專利範圍項數：10 項 圖式數：5 共 21 頁

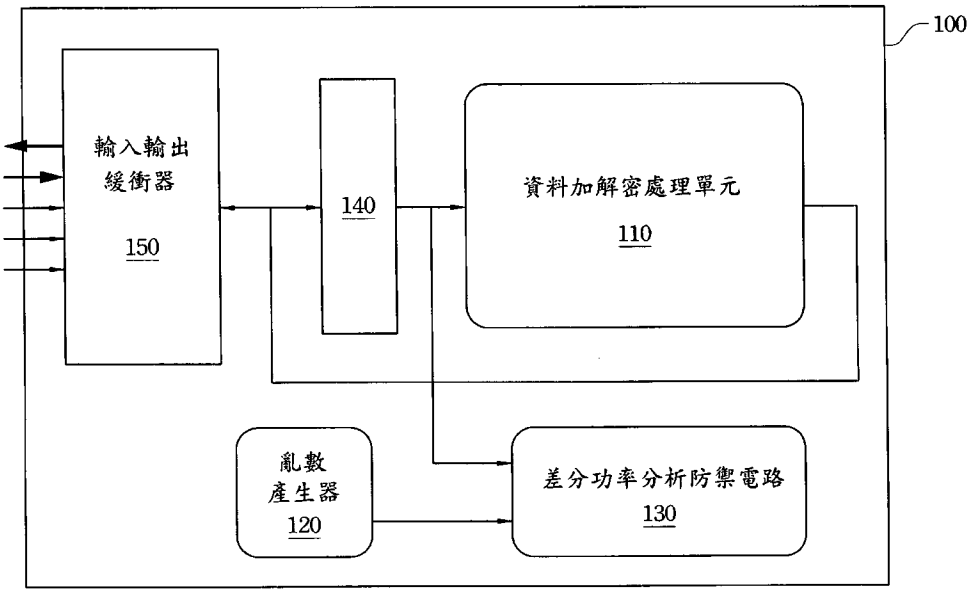
(54)名稱

防禦差分功率分析攻擊之方法及電子裝置

ELECTRONIC DEVICE AND METHOD FOR PROTECTING AGAINST DIFFERENTIAL POWER ANALYSIS ATTACK

(57)摘要

一種電子裝置包括一資料加解密處理單元、一亂數產生器與一差分功率分析防禦電路。資料加解密處理單元在進行加密或解密複數位元之資料時，可提供一致能訊號，亂數產生器可產生亂數資料。差分功率分析防禦電路在接收到致能訊號時，可依據這些位元之資料及亂數資料而運作。



100：電子裝置
110：資料加解密處理單元
120：亂數產生器
130：差分功率分析防禦電路
140：資料暫存器
150：輸入輸出緩衝器

201225613

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：99144013

※申請日：99.12.15 ※IPC 分類：H04L 9/00 (2006.01)

一、發明名稱：（中文/英文）

防禦差分功率分析攻擊之方法及電子裝置

Electronic Device and Method for Protecting against Differential Power Analysis Attack

二、中文發明摘要：

一種電子裝置包括一資料加解密處理單元、一亂數產生器與一差分功率分析防禦電路。資料加解密處理單元在進行加密或解密複數位元之資料時，可提供一致能訊號，亂數產生器可產生亂數資料。差分功率分析防禦電路在接收到致能訊號時，可依據這些位元之資料及亂數資料而運作。

三、英文發明摘要：

An electronic device and a method for protecting against differential power analysis attack are disclosed herein. The electronic device includes an encryption/decryption unit, a random number generator and a countermeasure circuit. The encryption/decryption unit can provide an enable signal when encrypting or decrypting more bits of data. The random number generator can generate random data. When receiving the enable signal, the countermeasure circuit can operate according the bits of data and the random data.

四、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100：電子裝置

110：資料加解密處理單元

120：亂數產生器

130：差分功率分析防禦電路

140：資料暫存器

150：輸入輸出緩衝器

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

[S]

六、發明說明：

【發明所屬之技術領域】

本發明是有關於一種方法及裝置，且特別是有關於一種防禦差分功率分析之方法及電子裝置。

【先前技術】

資料加解密演算法被廣泛地應用在無線通訊系統如無線區域網路、近場通訊以及資料儲存系統與銀行系統裡。而在 1999 年由 Paul Kocher 等人所發表差分功率分析（differential power analysis, DPA）能夠有效率地且低成本地針對加解密晶片進行破解，因此如何在加解密晶片中加入抵抗差分功率分析攻擊的機制為加解密系統設計上之重要考量。

所謂的差分功率分析攻擊法就是利用硬體在加、解密時，通道上所洩露的功率資訊來推導出秘密金鑰。當功率的消耗是與處理的資料有關且此資料是含有金鑰的資訊，那麼中間值的漢明差值與功率消耗就會有相關性存在。

由此可見，上述現有的資料保護機制，顯然仍存在不便與缺陷，而有待加以進一步改進。為了解決上述問題，相關領域莫不費盡心思來謀求解決之道，但長久以來一直未見適用的方式被發展完成。因此，如何能有效地防禦差分功率分析攻擊，實屬當前重要研發課題之一，亦成爲當前相關領域亟需改進的目標。

【發明內容】

[S]

因此，本發明之一態樣是在提供一種防禦差分功率分析攻擊之方法及電子裝置。

依據本發明一實施例，一種電子裝置包括一資料加解密處理單元、一亂數產生器與一差分功率分析防禦電路。在結構上，亂數產生器電性耦接資料加解密處理單元，差分功率分析防禦電路電性耦接亂數產生器及資料加解密處理單元。於使用上，資料加解密處理單元在進行加密或解密複數個位元之資料時，可提供一致能訊號，亂數產生器可產生亂數資料。差分功率分析防禦電路在接收到致能訊號時，可依據這些位元之資料及亂數資料而運作。

另一方面，資料加解密處理單元在未進行加密或解密時，則停止提供致能訊號，俾使差分功率分析防禦電路停止運作。

上述之差分功率分析防禦電路包括複數個環型震盪器。於使用時，這些環型震盪器皆接收亂數資料，其中每一環型震盪器各自接收對應之每一位元之資料。

每一環型震盪器可包括一互斥或閘、一第一反及閘、至少一反相器與一第二反及閘。在結構上，互斥或閘之一輸入端用以接收對應之位元之資料，互斥或閘之另一輸入端用以接收亂數資料。第一反及閘之一輸入端連接互斥或閘之輸出端，至少一反相器之輸入端連接第一反及閘之輸出端。第二反及閘之一輸入端連接此至少一反相器之輸出端，第二反及閘之另一輸入端用以接收致能訊號，第二反及閘之輸出端連接第一反及閘之另一輸入端。

舉例來說，上述之至少一反相器的數量可為奇數個。

[S]

上述之電子裝置亦可包括一資料暫存器與一輸入輸出緩衝器。在結構上，資料暫存器電性耦接資料加解密處理單元，輸入輸出緩衝器電性耦接資料暫存器。

在配置方面，上述之資料加解密處理單元、亂數產生器、差分功率分析防禦電路、輸入輸出緩衝器與資料暫存器皆設置於單一密碼晶片內。

依據本發明另一實施例，一種用於防禦差分功率分析之方法，此方法包含下列步驟：首先，在進行加密或解密複數個位元之資料時，產生一致能訊號，並產生亂數資料。接著，根據致能訊號以啟動一差分功率分析防禦電路，使差分功率分析防禦電路依據這些位元之資料及亂數資料而運作。

另一方面，當未進行加密或解密時，則停止提供致能訊號，俾使差分功率分析防禦電路停止運作。

綜上所述，本發明之技術方案與現有技術相比具有明顯的優點和有益效果。藉由上述技術方案，可達到相當的技術進步，並具有產業上的廣泛利用價值，其至少具有下列特點：

1. 動態地改變電子裝置在運算過程中的功率消耗特性，以降低電子裝置功率消耗與攻擊用之功率模型之間的相關性來達到抵抗 DPA 攻擊的目的；

2. 差分功率分析防禦電路以平行掛載之方式與資料加解密處理單元同時運作，以避免影響資料加解密處理單元原本之效能；以及

3. 以一致能訊號作為啟動控制，能讓此差分功率分析

[S]

防禦電路在電子裝置不需保護時停止運作以降低功率消耗。

以下將以實施方式對上述之說明作詳細的描述，並對本發明之技術方案提供更進一步的解釋。

【實施方式】

為了使本發明之敘述更加詳盡與完備，可參照所附之圖式及以下所述各種實施例，圖式中相同之號碼代表相同或相似之元件。另一方面，眾所週知的元件與步驟並未描述於實施例中，以避免對本發明造成不必要的限制。

於實施方式與申請專利範圍中，涉及『耦接(coupled with)』之描述，其可泛指一元件透過其他元件而間接連接至另一元件，或是一元件無須透過其他元件而直接連接至另一元件。

於實施方式與申請專利範圍中，除非內文中對於冠詞有所特別限定，否則『一』與『該』可泛指單一個或複數個。

本文中所使用之『約』、『大約』或『大致』係用以修飾任何可些微變化的數量，但這種些微變化並不會改變其本質。於實施方式中若無特別說明，則代表以『約』、『大約』或『大致』所修飾之數值的誤差範圍一般是容許在百分之二十以內，較佳地是於百分之十以內，而更佳地則是於百分五之以內。

本發明之技術態樣是一種電子裝置，其可在加解密時有效防禦差分功率分析攻擊，或是廣泛地運用在相似之技

[S]

術環節。以下將搭配第 1 圖來說明此電子裝置之具體實施方式。

參照第 1 圖，第 1 圖是依照本發明一實施例之一種電子裝置 100 的方塊圖。如第 1 圖所示，電子裝置 100 包括資料加解密處理單元 110、亂數產生器 120 與差分功率分析防禦電路 130。

在結構上，亂數產生器 120 電性耦接資料加解密處理單元 110，差分功率分析防禦電路 130 電性耦接亂數產生器 120 及資料加解密處理單元 110。

於使用上，資料加解密處理單元 110 在進行加密或解密複數個位元之資料時，可提供一致能訊號，亂數產生器 120 可產生亂數資料。差分功率分析防禦電路 130 在接收到致能訊號時，可依據這些位元之資料及亂數資料而運作，藉此動態地改變電子裝置 100 在運算過程中的功率消耗特性，以降低電子裝置 100 功率消耗與攻擊用之功率模型之間的相關性來達到抵抗 DPA 攻擊的目的。而且，差分功率分析防禦電路 130 係以平行掛載之方式與資料加解密處理單元 110 同時運作，可避免影響資料加解密處理單元 110 原本之效能。

另一方面，資料加解密處理單元 110 在未進行加密或解密時，則停止提供致能訊號，俾使差分功率分析防禦電路 130 停止運作。藉此，讓差分功率分析防禦電路 130 在電子裝置 100 不需保護時停止運作以降低功率消耗。

電子裝置 100 亦可包括資料暫存器 140 與輸入輸出緩衝器 150。在結構上，資料暫存器 140 電性耦接資料加解

密處理單元 110，輸入輸出緩衝器 150 電性耦接資料暫存器 140。於使用上，外部之複數位元之資料可透過輸入輸出緩衝器 150 傳輸至資料暫存器 140，而資料加解密處理單元 110 及差分功率分析防禦電路 130 可以自資料暫存器 140 取得資料。經資料加解密處理單元 110 加解密之資料亦可透過輸入輸出緩衝器 150 輸出到外部。

在配置方面，上述之資料加解密處理單元 110、亂數產生器 120、差分功率分析防禦電路 130、資料暫存器 140 與輸入輸出緩衝器 150 皆設置於單一密碼晶片內，亦即電子裝置 100 可為單一密碼晶片，藉此駭客難以用差分電力分析攻擊法，來竊取密碼晶片中之加解密資料。

實作上，資料加解密處理單元 110 可為資料處理電路、資料處理模組或類似裝置，熟習此項技藝者應視當時需要彈性選擇之。而關於差分功率分析防禦電路 130 之具體構造，請參照第 2 圖，第 2 圖是依照本發明一實施例之差分功率分析防禦電路 130 的電路方塊圖。

如第 2 圖所示，差分功率分析防禦電路 130 包括複數個環型震盪器 200。於使用上，這些環型震盪器 200 皆接收亂數資料，其中每一環型震盪器 200 各自接收每一位元之資料。藉此，以數位控制之環型振盪器 200 為基礎之差分功率分析防禦電路 130，搭配亂數產生器 120 產生之亂數資料來動態改變環型振盪器 200 的運作，達成改變電子裝置 100 功率消耗特性之目的。

每一環型震盪器 200 可包括互斥或閘 210、第一反及閘 220、反相器 230 與第二反及閘 240。在結構上，互斥或

閘 210 之一輸入端用以接收對應之位元之資料，互斥或閘之另一輸入端用以接收亂數資料。第一反及閘 220 之一輸入端連接互斥或閘之輸出端，反相器 230 之輸入端連接第一反及閘 220 之輸出端。第二反及閘 240 之一輸入端連接反相器 230 之輸出端，第二反及閘 240 之另一輸入端(init)用以接收致能訊號，第二反及閘 240 之輸出端連接第一反及閘 220 之另一輸入端。

雖然第 2 圖僅繪示單一個反相器 230，然此並不限制本發明，實作上，反相器230之數量為奇數個(如 1, 3, 5, 7,... 等等)即可，其中當反相器的數量為 3 個以上時，這些反相器係串接在一起以達到保護目的，熟習此項技藝者應視當時需要彈性選擇反相器 230 的實際數目。

如此，每一環型震盪器 200 可由一位元之資料以及一位元之隨機位元（即，上述之亂數資料）所控制，藉此動態改變電子裝置 100 功率消耗特性。而 init 為一啟動控制，能讓差分功率分析防禦電路 130 在電子裝置 100 不需保護時停止運作以降低功率消耗。

於第 2 圖中，使用較少的邏輯閘即可組成環型震盪器 200，藉以減少差分功率分析防禦電路 130 所佔用的面積、降低功耗，又足以防禦差分功率分析攻擊。雖然第 2 圖之電路有諸多優點，然此並不限制本發明，實作上，任何適用之環型震盪器架構皆可應用在差分功率分析防禦電路 130，熟習此項技藝者應視當時需要彈性設計之。

另一方面，於一實施例中，如第 1 圖所示之亂數產生器 120 基本上亦可由環型震盪器組成。舉例來說，亂數產

[S]

生器 120 可為環型震盪器式亂數產生器（ring oscillator based random number generator）。若亂數產生器 120 與差分功率分析防禦電路 130 主要皆由環型震盪器組成，可有利於製程上的設計。或者，於另一實施例中，亂數產生器 120 可採用其他亂數生成電路或隨機數產生機制，熟習此項技藝者可視實際需要，彈性選擇亂數產生器 120 的具體實施方式。

綜上所述，一種用於防禦差分功率分析攻擊之方法可包含下列步驟（應瞭解到，在本實施例中所提及的步驟，除特別敘明其順序者外，均可依實際需要調整其前後順序，甚至可同時或部分同時執行），至於實施該些步驟的硬體裝置，由於上述實施例已具體揭露，因此不再重複贅述之。

首先，在進行加密或解密複數個位元之資料時，產生一致能訊號，並產生亂數資料。接著，根據致能訊號以啟動一差分功率分析防禦電路，使差分功率分析防禦電路依據這些位元之資料及亂數資料而運作。

另一方面，於此方法中，當未進行加密或解密時，則停止提供致能訊號，俾使差分功率分析防禦電路停止運作。

第 3 圖是依照本發明一實施例之差分功率分析攻擊流程之示意圖。在應用上，上述之電子裝置 100 為一密碼晶片，密碼晶片接收使用者之明文／密文後以晶片內部之金鑰（key）進行加密／解密之運算，攻擊者可以透過所輸入之明文／密文與所有可能之金鑰假設建立一功率消耗模型 300 進行分析以破解金鑰。以 AES 加解密晶片為例，其分

[S]

析結果如第 4 圖所示，大約經過 9200 組運算後，正確金鑰所假設的功率消耗模型與晶片功率消耗的相關性即可大於其他金鑰，而 128 位元 AES 每次以 8 位元為單位，透過 16 次不同的分析便可破解出 128 位元之金鑰。

如第 5 圖所示為以本發明所提出之方法進行差分功率分析攻擊之防禦，其安全度可提高到至少 10,000,000 組運算仍無法破解出正確之金鑰。

雖然本發明已以實施方式揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作各種之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

為讓本發明之上述和其他目的、特徵、優點與實施例能更明顯易懂，所附圖式之說明如下：

第 1 圖是依照本發明一實施例之一種電子裝置的方塊圖；以及

第 2 圖是第 1 圖之差分功率分析防禦電路的電路方塊圖；

第 3 圖是依照本發明一實施例之差分功率分析攻擊流程之示意圖；

第 4 圖是未防禦差分功率分析攻擊所得之分析結果；以及

第 5 圖是以本發明所提出之方法去防禦差分功率分析攻擊之所得之分析結果。

[S]

【主要元件符號說明】

100：電子裝置

110：資料加解密處理單元

120：亂數產生器

130：差分功率分析防禦電路

140：資料暫存器

150：輸入輸出緩衝器

200：環型震盪器

210：互斥或閘

220：第一反及閘

230：反相器

240：第二反及閘

300：功率消耗模型

[S]

七、申請專利範圍：

1. 一種電子裝置，包含：

一資料加解密處理單元，用以在進行加密或解密複數位元之資料時，提供一致能訊號；

一亂數產生器，電性耦接該資料加解密處理單元，用以產生亂數資料；以及

一差分功率分析防禦電路，電性耦接該亂數產生器及該資料加解密處理單元，用以在接收到該致能訊號時，依據該些位元之位元之資料及該亂數資料而運作。

2. 如請求項 1 所述之電子裝置，其中該資料加解密處理單元在未進行加密或解密時，則停止提供該致能訊號，俾使該差分功率分析防禦電路停止運作。

3. 如請求項 1 所述之電子裝置，其中該差分功率分析防禦電路包含：

複數個環型震盪器，皆接收該亂數資料，其中每一環型震盪器各自接收對應之每一該位元之資料。

4. 如請求項 3 所述之電子裝置，其中每一該環型震盪器包含：

一互斥或閘，該互斥或閘之一輸入端用以接收對應之該位元之資料，該互斥或閘之另一輸入端用以接收該亂數

[S]

資料；

一第一反及閘，該第一反及閘之一輸入端連接該互斥或閘之輸出端；

至少一反相器，該至少一反相器之輸入端連接該第一反及閘之輸出端；

一第二反及閘，該第二反及閘之一輸入端連接該至少一反相器之輸出端，該第二反及閘之另一輸入端用以接收該致能訊號，該第二反及閘之輸出端連接該第一反及閘之另一輸入端。

5. 如請求項 4 所述之電子裝置，其中該至少一反相器之數量為奇數個。

6. 如請求項 1 所述之電子裝置，更包含：

一資料暫存器，電性耦接該資料加解密處理單元；以及

一輸入輸出緩衝器，電性耦接該資料暫存器。

7. 如請求項 6 所述之電子裝置，其中該資料加解密處理單元、該亂數產生器、該差分功率分析防禦電路、該輸入輸出緩衝器與資料暫存器該皆設置於單一密碼晶片內。

8. 如請求項 1 所述之電子裝置，其中該亂數產生器基本上由環型震盪器組成。

[S]

9. 一種用於防禦差分功率分析（differential power analysis）攻擊之方法，該方法包含：

在進行加密或解密複數位元之資料時，產生一致能訊號；

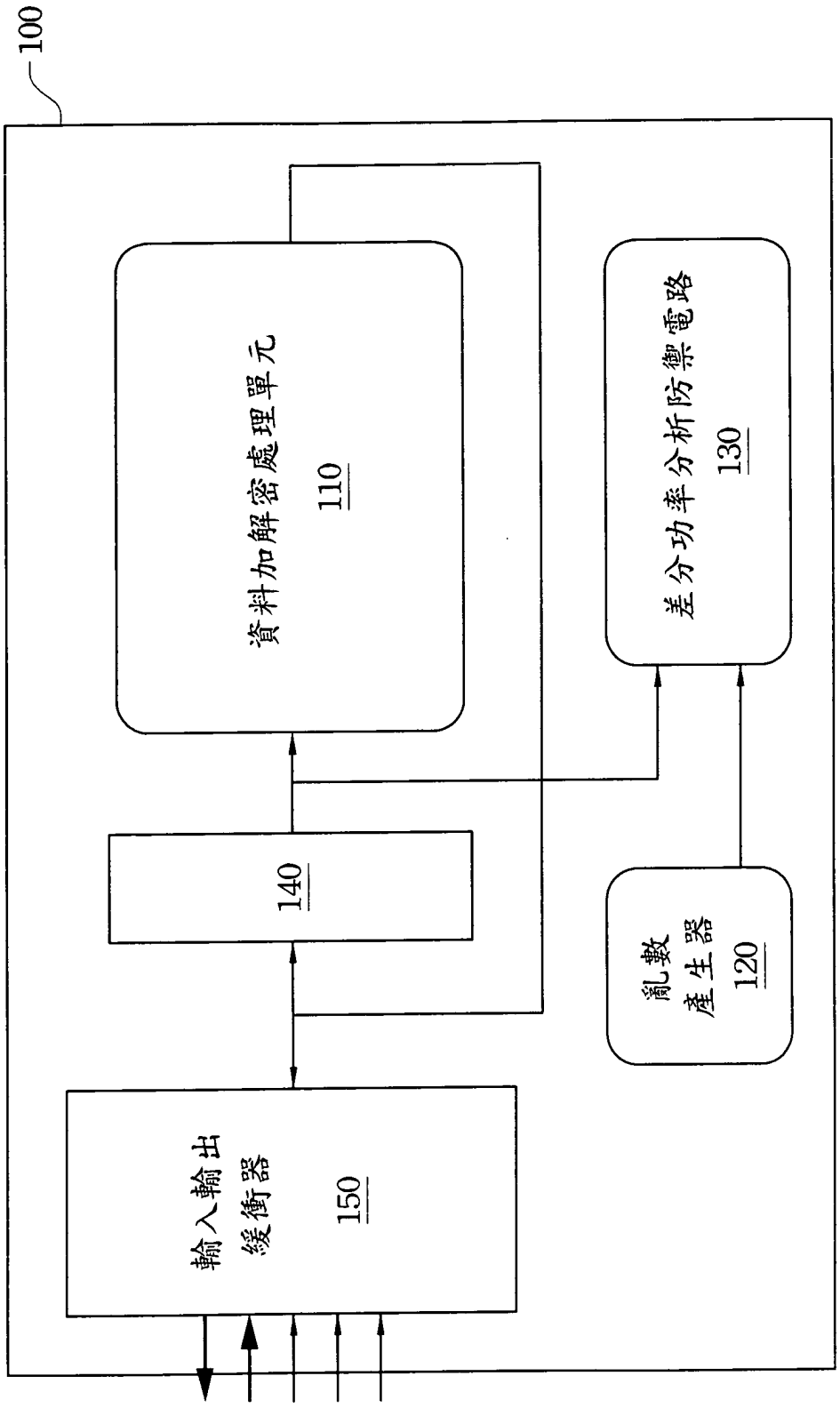
產生亂數資料；以及

根據該致能訊號以啟動一差分功率分析防禦電路，使該差分功率分析防禦電路依據該些位元之資料及該亂數資料而運作。

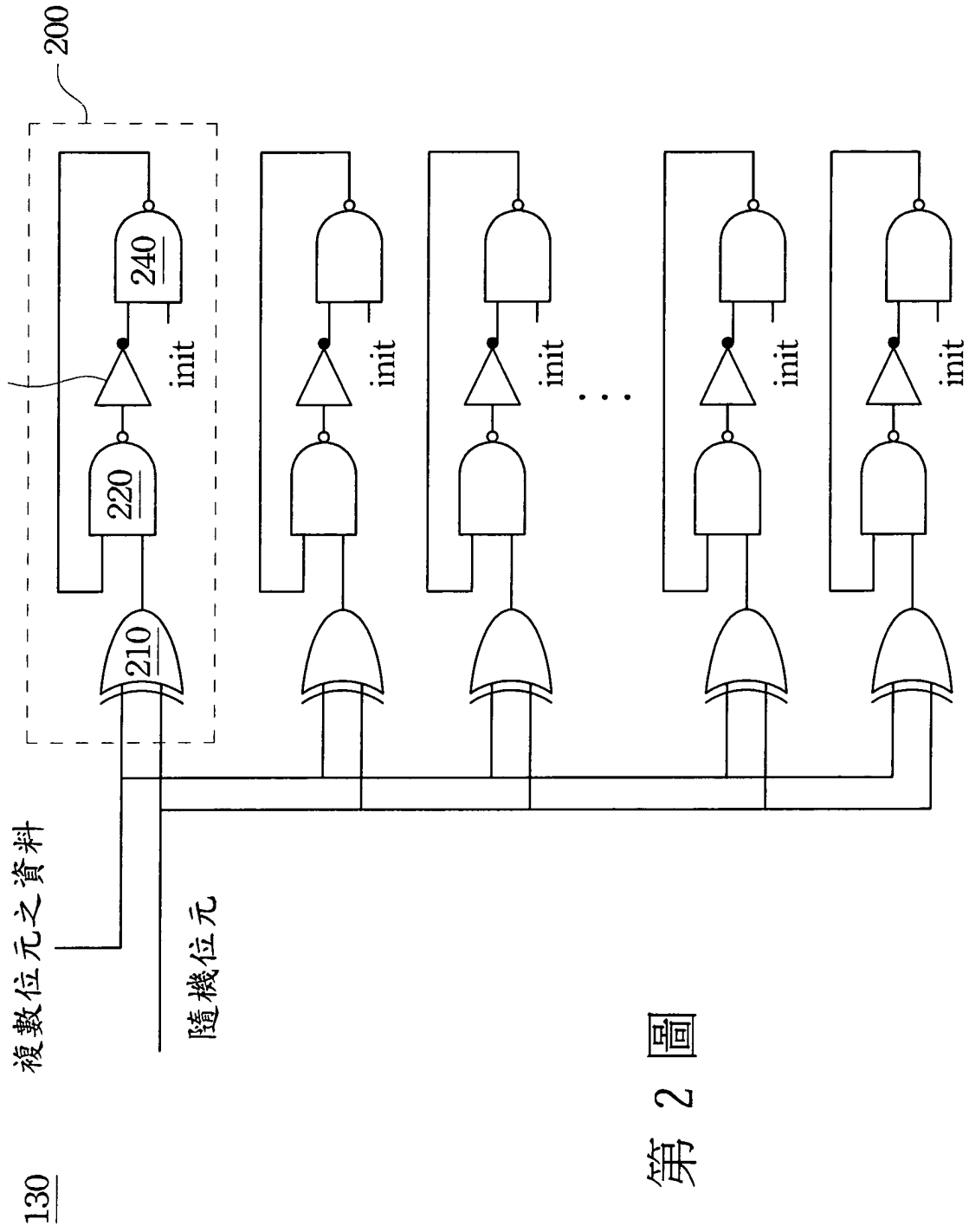
10. 如請求項9所述之方法，更包含：

當未進行加密或解密時，則停止提供該致能訊號，俾使該差分功率分析防禦電路停止運作。

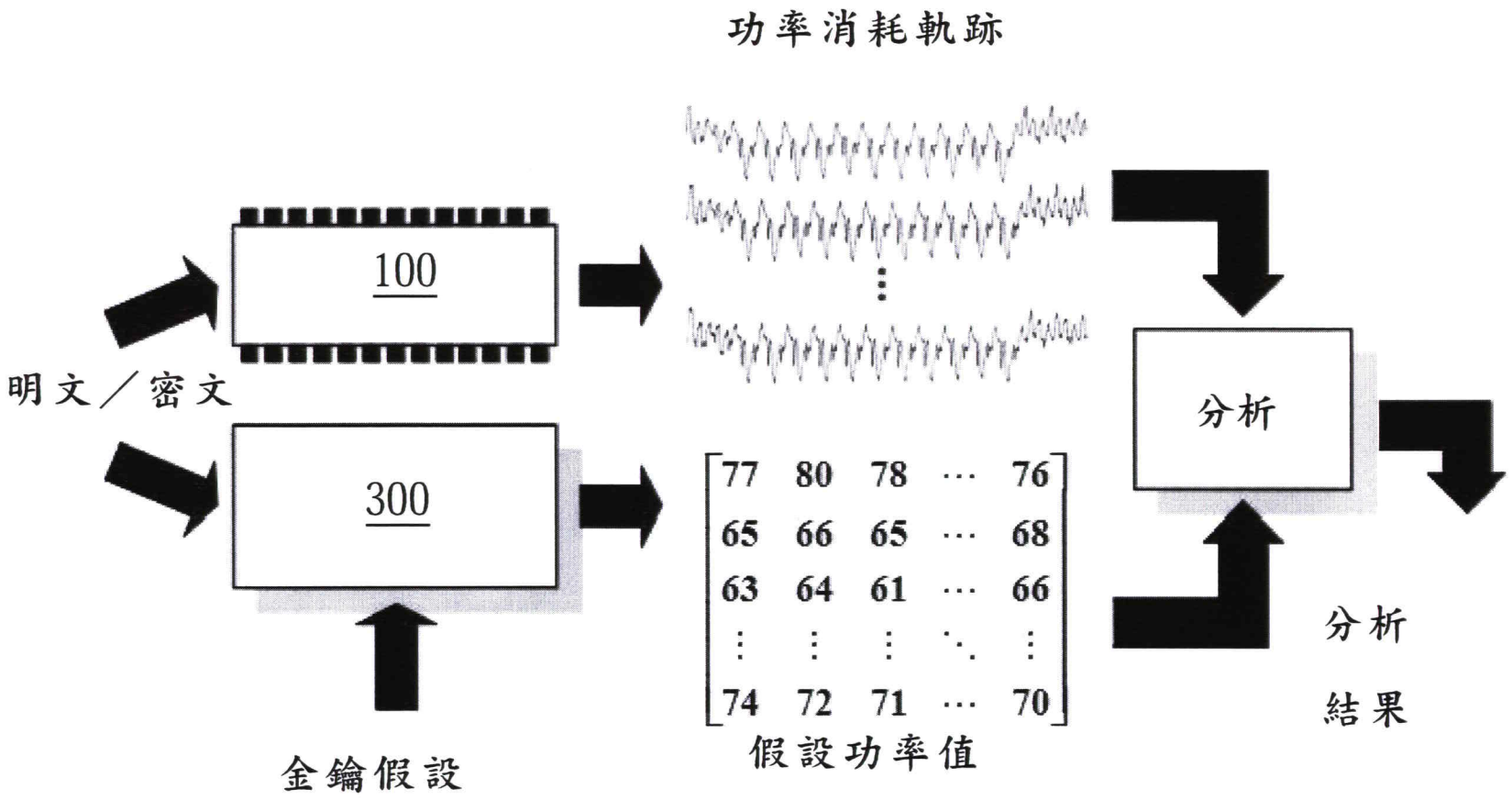
[S]



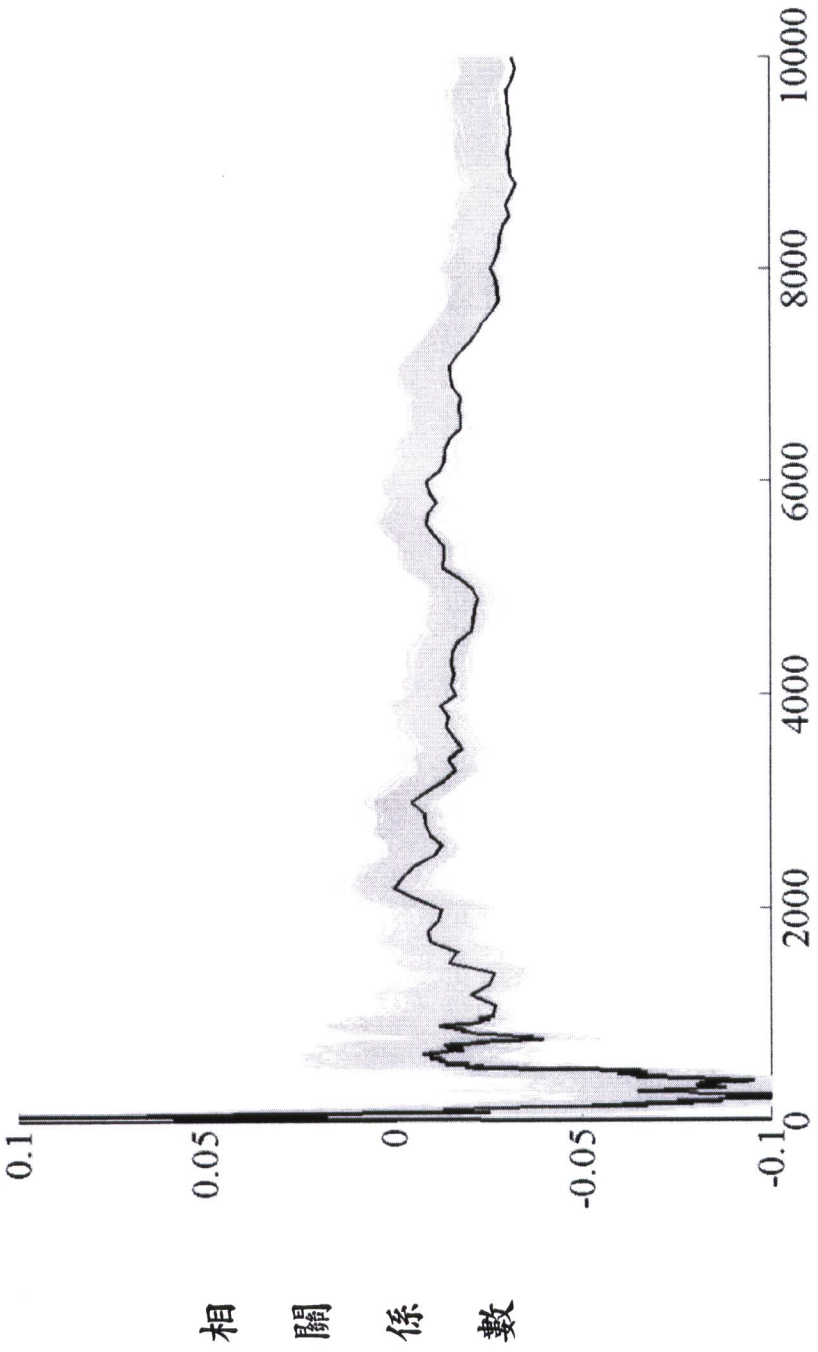
第 1 圖



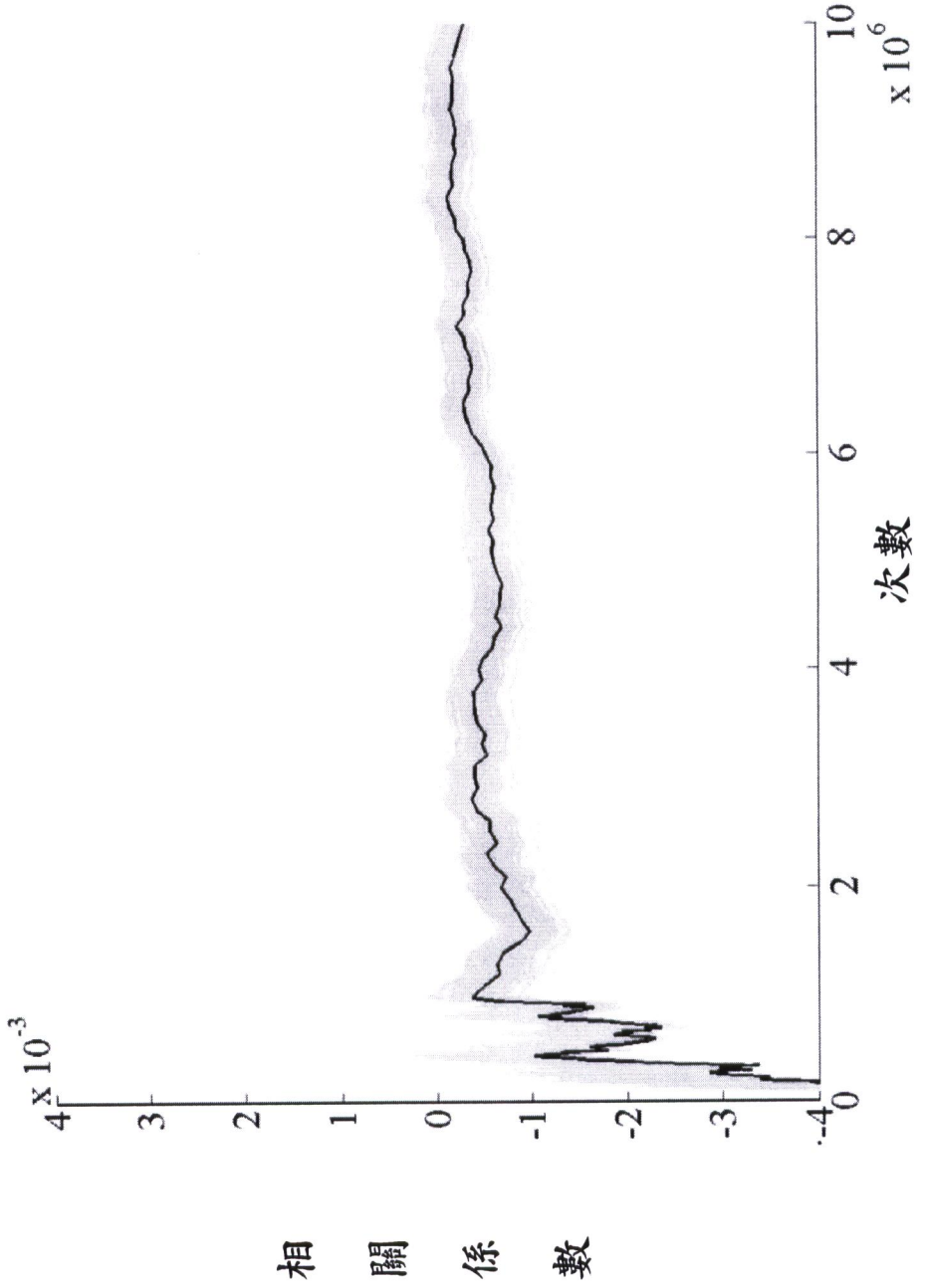
第 2 圖


功率消耗軌跡
100
明文／密文
300
金鑰假設
77 80 78 … 76
65 66 65 … 68
63 64 61 … 66
74 72 71 … 70
假設功率值
分析
分析
結果

第 3 圖



第 4 圖



第 5 圖