I533652

(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 I533652 B**

(45)公告日： 中華民國 105 (2016) 年 05 月 11 日

(21)申請案號：103100515 (22)申請日： 中華民國 103 (2014) 年 01 月 07 日

(51)Int. Cl.： ***H04L9/06*** ***(2006.01)*** ***H04L9/08*** ***(2006.01)***

(30)優先權：2013/01/11 美國 61/751,541

2013/07/05 美國 13/935,962

(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：羅斯 葛格利 高登 ROSE, GREGORY GORDON (AU)

(74)代理人：陳長文

(56)參考文獻：

CN 101729241A US 4382300

US 2002/0154767A1 US 2008/0019503A1

US 2008/0212776A1 US 2010/0329450A1

WO 99/08411

Qin Zhongping, Yang Qi, Zhai Li, "Optimization of S-Boxes by Evolving", Intelligent Systems and Applications (ISA), 2010 2nd International Workshop on, 22-23 May 2010,

審查人員：陳怡婷

申請專利範圍項數：28 項 圖式數：11 共 41 頁

(54)名稱

用於可計算、大型、可變及安全的替換盒之方法及裝置

METHOD AND APPARATUS FOR A COMPUTABLE, LARGE, VARIABLE AND SECURE SUBSTITUTION BOX

(57)摘要

一特徵關於一種用於產生與替換盒(S 盒)相關聯之加密值的方法。該方法包括首先獲得一輸入值及一第一值。一方法包括藉由以下步驟來產生一 S 盒輸出值：對該輸入值及該第一值執行一互斥或(XOR)操作以產生一中間值，且對該中間值以等於該中間值之漢明權重的一位元數目執行一逐位元旋轉。在一態樣中，此逐位元旋轉之輸出與一第二值進一步進行 XOR。另一方法包括藉由以下步驟來產生該 S 盒輸出值：對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉以產生一中間值，且對該中間值及該第一值執行一 XOR 操作。

One feature pertains to methods for generating cryptographic values associated with substitution boxes (S-box). The methods includes first obtaining an input value and a first value. One method includes generating an S-box output value by performing an exclusive OR (XOR) operation on the input value and the first value to generate an intermediate value, and performing a bitwise rotation on the intermediate value by a number of bits equal to the Hamming Weight of the intermediate value. In one aspect, the output of this bitwise rotation is further XOR-ed with a second value. Another method includes generating the S-box output value by performing a bitwise rotation on the input value by a number of bits equal to the Hamming

Weight of the input value to generate an intermediate value, and performing an XOR operation on the intermediate value and the first value.

指定代表圖：

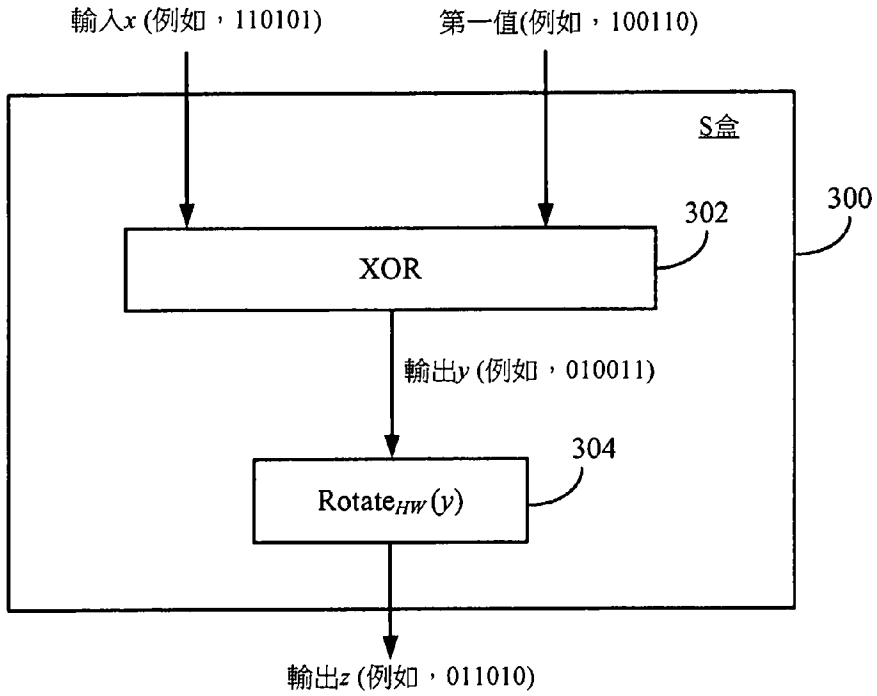

圖3

符號簡單說明：

300・・・替換盒(S盒)

302・・・逐位元互斥或(XOR)函數

304・・・旋轉函數

公告本

發明摘要

※ 申請案號：102100515

※ 申請日： 102.1.7 ※IPC 分類：

H04L 9/06 (2006.01)

9/08 (2006.01)

【發明名稱】

用於可計算、大型、可變及安全的替換盒之方法及裝置

METHOD AND APPARATUS FOR A COMPUTABLE, LARGE, VARIABLE AND SECURE SUBSTITUTION BOX

【中文】

一特徵關於一種用於產生與替換盒(S盒)相關聯之加密值的方法。該方法包括首先獲得一輸入值及一第一值。一方法包括藉由以下步驟來產生一S盒輸出值：對該輸入值及該第一值執行一互斥或(XOR)操作以產生一中間值，且對該中間值以等於該中間值之漢明權重的一位元數目執行一逐位元旋轉。在一態樣中，此逐位元旋轉之輸出與一第二值進一步進行XOR。另一方法包括藉由以下步驟來產生該S盒輸出值：對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉以產生一中間值，且對該中間值及該第一值執行一XOR操作。

【英文】

One feature pertains to methods for generating cryptographic values associated with substitution boxes (S-box). The methods includes first obtaining an input value and a first value. One method includes generating an S-box output value by performing an exclusive OR (XOR) operation on the input value and the first value to generate an intermediate value, and performing a bitwise rotation on the intermediate value by a number of bits equal to the Hamming Weight of the intermediate value. In one aspect, the output of this bitwise rotation is further XOR-ed with a second value. Another method includes generating the S-box output value by performing a bitwise rotation on the input value by a number of bits equal to the Hamming Weight of the input value to generate an intermediate value, and performing an XOR operation on the intermediate value and the first value.

【代表圖】

【本案指定代表圖】：第（3）圖。

【本代表圖之符號簡單說明】：

300　　替換盒(S盒)

302　　逐位元互斥或(XOR)函數

304　　旋轉函數

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】

用於可計算、大型、可變及安全的替換盒之方法及裝置

METHOD AND APPARATUS FOR A COMPUTABLE, LARGE, VARIABLE AND SECURE SUBSTITUTION BOX

優先權之主張

本專利申請案主張2013年1月11日申請的標題為「Method and Apparatus for Computable, Large, Variable, and Secure Substitution Box」之臨時申請案第61/751,541號的優先權，該申請案之全部揭示內容特此以引用的方式明確地併入。

【技術領域】

各種特徵係關於密碼學，且更確切而言係關於用於實施替換盒之方法及裝置。

【先前技術】

在密碼學中，替換盒(S盒)為執行替換之對稱金鑰演算法的基本組件。在區塊密碼中，區塊密碼通常用以隱藏金鑰與密文之間的關係，且因此展現向農的混淆之性質。S盒表示接收*n*個輸入位元且產生*m*個輸出位元的複合函數，從而輸出具有某些用於加密之性質。此等性質包括高非線性與平衡性、高代數次數、嚴格雪崩準則滿足程度，及其他性質。此等函數難以計算，且常常表示為查找表，諸如資料加密標準(DES)及進階加密標準(AES)中的查找表。舉例而言，在AES中，8位元輸入藉由選自S盒中之8位元值替換。在一些狀況下，*n*可等於*m*，從而至S盒之輸入及輸出具有相同位元長度。

若*n*大，則上文描述之查找表(或等效地，用於硬體實施之閘的網

路)可快速變得不實用。在另一方面，小n在定義上限於非線性及代數次數。因此，亦能夠有效實施於硬體或軟體中的具有大量輸入位元之S盒係合乎要求的。

隱藏權重位元函數(HWBF)可視為具有上文描述的一些合乎要求之加密性質(諸如平衡性及代數複雜性)的n位元至1位元S盒。舉例而言，若x為一n位元輸入，其中x_i為x之第i (1 <= i <= n)個最高有效位元，則HWBF之輸出W定義為：

若$x = 0$，則$W(x) = 0$，

否則，$W(x) = x_k$，其中k為x之漢明權重。

圖1說明可易於實施於硬體中之先前技術中出現的基於n位元至n位元HWBF之S盒100的示意性方塊圖。二進位輸入值x(例如，110101)被輸入至旋轉函數102中。旋轉函數102對輸入x以等於輸入之漢明權重的一位元數目執行逐位元左旋轉。因此，若二進位輸入x等於110101，則由於漢明權重等於四個(4)，因此旋轉函數102之輸出z等於011101。

圖2說明描繪基於HWBF之S盒輸出z與HWBF $W(x)$之間關係的表200。參看圖1及圖2，可展示，輸出z之最低有效位元(例如，1)等於輸入值x之HWBF $W(x)$(上文定義)。亦可觀察到，第二最低有效位元(例如，0)表示至HWBF之輸入值x已經歷單一位元的逐位元右旋轉(藉由$W(x<<1)$指示)之情況下的HWBF $W(x)$之輸出。第三最低有效位元表示至HWBF之輸入值x已經歷兩個位元的逐位元右旋轉(藉由$W(x<<2)$指示)之情況下的HWBF $W(x)$之輸出，等等。

因此，輸出值z與輸入值x具有相同數目之位元，其中每一位元表示並列計算出的不同HWBF $W(x)$輸出。輸出值z之位元仍保留上文關於HWBF描述的一些有益的加密性質。不幸的是，S盒100亦具有不合乎要求的性質。舉例而言，一此不合乎要求之性質在於輸出z將與輸

入x具有相同漢明權重，此可常常簡化密碼分析，特別在輸入x具有低漢明權重時。將需要增大S盒100之安全性，以使得更能抵抗密碼攻擊(密碼分析)。

因此，需要更有效地抵抗密碼攻擊的改良式S盒演算法、方法，及裝置。

【發明內容】

一特徵提供一種用於產生與一替換盒(S盒)相關聯之加密值的方法。該方法包含獲得一輸入值及一第一值，及藉由以下步驟中之一者產生一S盒輸出值：(A)對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值，且對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值；(B)對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該第一中間值，且對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值；或(C)對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值，對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生一第二中間值，獲得一第二值，且對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值。根據一態樣，所提供之該第一值及/或該第二值中的至少一者經組態以產生具有等於或大於50%可能性之與該輸入值具有一不同漢明權重的該S盒輸出值。根據另一態樣，該第一值及/或該第二值中的至少一者為具有一非零漢明權重的一常數。

根據一態樣，所提供之該第一值及/或該第二值中的至少一者係可變的，且具有等於或大於百分之100*(1 - 2^{-n})的具有一非零漢明權重之一可能性，其中n為該第一值及/或該第二值之一位元數目。根據另一態樣，該第一值及/或該第二值中的至少一者係自一加密函數及/

或加密金鑰中的至少一者導出。根據又一態樣，該第一值及/或該第二值中的至少一者係自一密碼模組的一組件級導出。

根據一態樣，該密碼模組係一流密碼。根據另一態樣，該方法係於一記憶體電路中執行。根據又一態樣，該輸入值及該S盒輸出值具有相同位元數目。

根據一態樣，該方法進一步包含：獲得一主要輸入值；分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及串接該複數個NLTF輸出值以獲得該輸入值。根據另一態樣，該主要輸入值經分配使得該複數個NLTF輸入值中之每一者具有相同位元數目。

另一特徵提供一種電子器件，該電子器件包含經組態以獲得一輸入值及一第一值，且藉由以下操作中之一者產生一S盒輸出值的一處理電路：(A)對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值，且對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值；(B)對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該第一中間值，且對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值；或(C)對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值，對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生一第二中間值，獲得一第二值，且對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值。

根據一態樣，該處理電路經進一步組態以：獲得一主要輸入

值；分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及串接該複數個NLTF輸出值以獲得該輸入值。

另一特徵提供一種電子器件，該電子器件包含用於獲得一輸入值及一第一值之構件，及用於藉由以下操作中之一者產生一S盒輸出值的構件：(A)用於對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值的構件，及用於對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值的構件；(B)用於對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作以產生該第一中間值的構件，及用於對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值的構件；或(C)用於對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值的構件，用於對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作以產生一第二中間值的構件，用於獲得一第二值的構件，及用於對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值的構件。

根據一態樣，該電子器件進一步包含：用於獲得一主要輸入值的構件；用於分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值的構件，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；用於將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值的構件，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及用於串接該複數個NLTF輸出值以獲得該輸入值的構件。

另一特徵提供一種電腦可讀儲存媒體，其具有儲存於其上之用於產生與一替換盒(S盒)相關聯之加密值的指令，該指令在藉由至少一處理器執行時使得該處理器獲得一輸入值及一第一值且藉由以下操作中之一者產生一S盒輸出值：(A)對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值，且對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作以產生該S盒輸出值；(B)對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作以產生該第一中間值，且對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值；或(C)對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值，對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作以產生一第二中間值，獲得一第二值，且對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值。

根據一態樣，該等指令在藉由該處理器執行時進一步使得該處理器：獲得一主要輸入值；分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及串接該複數個NLTF輸出值以獲得該輸入值。

【圖式簡單說明】

圖1說明先前技術中出現的基於n位元至n位元漢明權重位元函數(HWBF)之替換盒(S盒)的示意圖方塊圖。

圖2說明描繪基於HWBF之S盒輸出z與HWBF $W(x)$之間關係的表。

圖3說明S盒之第一例示性示意性方塊圖。

圖4說明S盒之第二例示性示意性方塊圖。

圖5說明S盒之第三例示性示意性方塊圖。

圖6說明加密函數f自加密金鑰/識別符K_1導出變值C_1的實例。

圖7說明自密碼模組之級導出/接收變值C_2的實例。

圖8說明S盒之第四例示性示意性方塊圖。

圖9說明用於產生與S盒相關聯之加密值之方法的流程框圖。

圖10說明合併上文描述之S盒的電子器件之硬體實施的示意性方塊圖。

圖11說明電子器件之處理器的示意性方塊圖。

【實施方式】

在以下說明中，給出具體細節以提供對本發明之各種態樣的完整理解。然而，一般熟習此項技術者應理解，可在無此等具體細節之情況下實踐該等態樣。舉例而言，可以方塊圖展示電路，以免以不必要之細節模糊該等態樣。在其他例項中，可不詳細展示熟知電路、結構及技術，以免模糊本發明之態樣。

詞語「例示性」在本文中用以意謂「充當一實例、例項或說明」。本文中描述為「例示性」的任何實施或態樣不必理解為比揭示內容之其他態樣較佳或有利。同樣，術語「態樣」不要求揭示內容之所有態樣包括所論述的特徵、優點或操作模式。

例示性S盒：對HWBF之輸入執行互斥或(XOR)操作

圖3說明根據本發明之一態樣的S盒300之示意性方塊圖。逐位元互斥或(XOR)函數302接收輸入值x(例如，110101)及第一值(例如，100110)作為輸入。在所說明之實例中，第一值為具有非零漢明權重之一常數值。逐位元XOR函數302產生輸入至旋轉函數304中之第一中間輸出y(例如，010011)。在此實例中，旋轉函數304對第一中間輸出y執行逐位元左旋轉，旋轉輸出y之漢明權重(例如，左旋轉3)。旋轉函

數304之所得輸出z(例如，011010)表示n個並列HWBF輸出，其中n為輸入值x之位元長度。應注意，輸出z不必與輸入值x具有相同漢明權重，且因此S盒300之輸出z相比先前技術方法在抵抗密碼分析方面更安全。S盒300之輸出z可與輸入x具有相同位元數目。根據一態樣，旋轉函數304可作為代替執行逐位元右旋轉，且過程將在加密安全性方面仍然等效。

XOR函數302可為充當用於對輸入值及第一值執行逐位元互斥或操作以產生第一中間值之構件的一實例的一XOR電路。旋轉函數304可藉由充當以下項之一實例的$\text{Rotate}_{\text{HM}}$電路執行：用於對第一中間值以等於第一中間值之漢明權重的位元數目執行逐位元旋轉操作，以產生S盒輸出值的構件；及用於產生輸出S盒值的構件。

例示性S盒：對HWBF之輸出執行XOR操作

圖4說明根據本發明之一態樣的S盒400之示意性方塊圖。旋轉函數402接收輸入值x(例如，110101)作為輸入。在此實例中，旋轉函數402對輸入值x執行逐位元左旋轉，旋轉輸入x之漢明權重(例如，左旋轉4)以產生第一中間輸出y(例如，011101)。旋轉函數402之所得中間輸出y表示n個並列HWBF輸出，其中n為輸入值x之位元長度。接下來，逐位元XOR函數404接收中間輸出y及第一值(例如，101100)作為輸入。在所說明之實例中，第一值為具有非零漢明權重之一常數值。XOR函數404產生不必與輸入值x具有相同漢明權重的輸出z(例如，110001)。因此S盒400之輸出z相比先前技術方法在抵抗密碼分析方面更安全。S盒400之輸出z可與輸入x具有相同位元數目。根據一態樣，旋轉函數402可作為代替執行逐位元右旋轉，且過程將在加密安全性方面仍然等效。

旋轉函數402可藉由$\text{Rotate}_{\text{HM}}$電路執行，該電路充當用於對輸入值以等於輸入值之漢明權重的位元數目執行逐位元旋轉操作，以產生

第一中間值之構件的一實例。XOR函數404可藉由充當以下項之一實例的XOR電路執行：用於對第一中間值及第一值執行逐位元XOR操作以產生S盒輸出值的構件；及用於產生輸出S盒值的構件。

例示性S盒：對HWBF之輸入及輸出執行XOR操作

圖5說明根據本發明之一態樣的S盒500之示意性方塊圖。逐位元XOR函數502接收輸入值x(例如，110101)及第一值(例如，001100)作為輸入。在所說明之實例中，第一值為具有非零漢明權重之一常數值。逐位元XOR函數502產生輸入至旋轉函數504中之第一中間輸出w(例如，111001)。在此實例中，旋轉函數504對第一中間輸出w執行逐位元左旋轉，旋轉輸出w之漢明權重(例如，左旋轉4)。旋轉函數504之所得第二中間輸出y(例如，011110)表示n個並列HWBF輸出，其中n為中間值y之位元長度。接著，另一逐位元XOR函數506接收第二中間輸出y及第二值(例如，111000)作為輸入。在所說明之實例中，第二值為具有非零漢明權重之一常數值。XOR函數506產生不必與輸入值x具有相同漢明權重的輸出z(例如，100110)。因此S盒500之輸出z相比先前技術方法在抵抗密碼分析方面更安全。S盒500之輸出z可與輸入x具有相同位元數目。根據一態樣，旋轉函數504可執行逐位元右旋轉作為代替，且過程將仍在加密上等效。

XOR函數502可藉由充當用於對輸入值及第一值執行逐位元XOR操作以產生第一中間值之構件的一實例的一XOR電路執行。旋轉函數504可藉由Rotate_{HM}電路執行，該電路充當用於對第一中間值以等於第一中間值之漢明權重的位元數目執行逐位元旋轉操作以產生第二中間值之構件的一實例。XOR函數506可藉由充當以下各者之一實例的XOR電路執行：對第二中間值及第二值執行逐位元XOR操作以產生S盒輸出值；及用於產生輸出S盒值的構件。

在上文關於圖3、圖4，及圖5描述之實例中，旋轉函數執行等於

其輸入之漢明權重的逐位元左旋轉。然而，在其他態樣中，旋轉函數可執行等於其輸入之漢明權重的逐位元右旋轉。在此狀況下，藉由旋轉函數輸出之值的最高有效位元(而非最低有效位元)表示替代性HWBF $W'(x)$之輸出。替代性HWBF $W'(x)$可具有輸入x，其為一n位元輸入，其中x_i為x之第i個最低有效位元($1 <= i <= n$)。函數$W'(x)$因此定義為：

若x = 0，則$W'(x) = 0$，

否則，$W'(x) = x_k$，其中k為x之漢明權重。

作為一實例，若旋轉函數504將第一中間值w 111001向右旋轉而非向左旋轉，則第二中間值y將等於100111而非011110。在進行第二值111000之XOR操作506之後，S盒500之輸出z將為011111。

根據一態樣，輸入至XOR函數302、404、502、506之第一及第二值可為如上文描述之常數。然而，在其他態樣中，第一及第二值完全無需為常數。在一態樣中，第一及第二值可為可變的，從而其值隨時間改變，在起動時改變，及/或在S盒300、400、500之某一迭代數目(亦即，所產生之輸出值)之後改變。作為一實例，第一及第二值可為可變的，此係因為該等值係使用改變之函數或本身改變之金鑰而自加密金鑰導出。此方案可使得S盒300、400、500之輸出對密碼攻擊更有效。根據一態樣，所提供之第一及/或第二值經組態以產生與輸入值具有不同漢明權重的S盒輸出值，其中可能性等於或大於50%。

第一與第二值之例示性類型

圖6說明加密函數f 602自加密金鑰/識別符K_I導出變值C_I的一此實例。除其他之外，加密函數f 602可為雜湊函數。變值C_I接著以上文關於圖3描述之相同方式用作輸入至XOR函數302中以產生S盒300輸出z的第一值。其他S盒400、500中的任一者可以相同方式進行修改，從而彼處使用之第一及/或第二值係使用加密函數自金鑰/識別符導出，

諸如加密函數f602及金鑰/識別符K_1。

根據第一與第二值可變的另一態樣，第一與第二值可自鄰近於S盒發生之加密的其他操作導出。圖7說明自密碼模組702之級導出/接收變值C_2的一此實例。密碼模組702可包括複數N個整數組件704、706、708，且變值C_2可自至彼等組件704、706、708中之任一者的輸出或輸入導出。除其他之外，組件704、706、708可為移位暫存器、加法器、乘法器、處理電路/區塊等等。在一態樣中，S盒300、400、500可為密碼模組702的部分，但在其他態樣中，S盒300、400、500可獨立於密碼模組702。根據一實例，密碼區塊702可為流密碼。

變值$C2$接著以上文關於圖3描述之相同方式用作輸入至XOR函數302中以產生S盒300輸出z的第一值。其他S盒400、500中的任一者可以相同方式進行修改，從而彼處使用之第一及/或第二值係如圖7中所示的自密碼模組之一或多級導出。

根據一態樣，可變輸入C_1與C_2(亦即，第一與第二值)可經提供從而具有等於或大於50%、60%、70%、80%、90%、95%，或99%中之一者的具有非零漢明權重之可能性。根據另一態樣，可變輸入C_1與C_2可經提供從而具有等於或大於百分之100*(1-2^{-n})的具有非零漢明權重之可能性，其中n為可變輸入C_1與C_2之位元數目。

特徵為額外NLTF級之例示性S盒

圖8說明根據本發明之另一態樣的S盒800之示意性方塊圖。S盒800(例如，「主要S盒」)包含位元分配電路802、複數N個非線性變換函數(NLTF)子電路804、806、808、810(其中N為等於或大於兩個(2)的整數)、串接電路812，及S盒A子電路814。非NLTF子電路804、806、808、810可為基於標準非線性變換表的s盒。S盒子電路A 814為圖3至圖7中展示且描述之S盒300、400、500中的任一者。

主要S盒800接收n位元主要輸入x且產生改良加密安全性的n位元

主要S盒輸出z。位元分配電路802將n位元主要輸入x碎裂成複數個較小的m_1、m_2、m_3、……、m_N位元NLTF輸入值803a、803b、803c、……、803n(亦即，m_1、m_2、m_3及m_N小於n)。非NLTF子電路804、806、808、810可根據非線性操作，使用查找表將NLTF輸入值803a、803b、803c、……、803n變換成NLTF輸出值805a、805b、805c、……、805n。NLTF輸入值803a、803b、803c、……、803n可與其對應的NLTF輸出值805a、805b、805c、……、805n具有相同位元數目。NLTF輸出值805a、805b、805c、……、805n接著藉由串接電路812串接在一起以產生n位元輸入值y。與上文關於圖3至圖7描述之操作/步驟相同，S盒A 804連同第一及/或第二值接收n位元輸入值y(參見，例如圖3至圖7)，且執行一或多個XOR及漢明權重旋轉操作(參見，例如圖3至圖7)以產生主要n位元S盒輸出值z。此等輸出值可與藉由S盒子電路804、806、808、810接收之輸入值具有相同位元長度(亦即，m_1、m_2、m_3及m_N)。

根據一態樣，位元分配電路802充當用於分配主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值之構件的一實例，其中每一NLTF輸入值具有小於主要輸入值之位元數目的一位元數目。位元分配電路802可進一步充當用於將NLTF輸入值中之每一者提供至執行非線性操作的NLTF以產生複數個NLTF輸出值之構件的一實例，其中該複數個NLTF輸出值中的每一者對應於提供至NLTF之NLTF輸入值。串接電路812充當用於串接複數個NLTF輸出值以獲得輸入值之構件的一實例。

現將根據一非限制性實例描述主要S盒800之操作。主要S盒800可接收具有位元b_0、b_1、b_2、…、b_{31}之一32位元主要輸入x，其中位元分配電路802將該32位元主要輸入碎裂成至NLTF子電路804、806、808、810的四個(4) 8位元輸入803a、803b、803c、…、803n。四個(4)

8位元輸入803a、803b、803c、…、803n可因此藉由位元表示：b_0, b_1, b_2, … b_7；b_8, b_9, b_{10}, … b_{15}；b_{16}, b_{17}, b_{18}, … b_{23}；及b_{24}, b_{25}, b_{26}, … b_{31}。每一NLTF子電路804、806、808、810接收其對應輸入，且可產生相等位元數目(例如，8位元)之輸出805a、805b、805c、…、805n。串接電路812接著串接此等輸出值805a、805b、805c、…、805n以產生32位元S盒A 814輸入值y。根據一態樣，值m_1、m_2、m_3，及m_N彼此相等，從而來自主要輸入x之相等數目之位元被發送至每一NLTF子電路804、806、808、810。根據另一態樣，值m_1、m_2、m_3，及m_N彼此不等，但小於位元數目值n。

根據一實例，S盒A 814為圖3中所示之S盒300。因此，類似於圖3中描繪之過程，S盒A 814對輸入值y及32位元第一值執行XOR操作以產生中間值。接下來，S盒A 814將中間值旋轉(左或右)中間值之漢明權重。接著，所得的經旋轉32位元值作為32位元主要S盒輸出值z自S盒A 814輸出。32位元第一值可藉由電路提供(圖8中未展示)，且可為常數(如圖3中所示)或變數(如圖6及圖7中所示)。

用於產生加密值之例示性方法

圖9說明用於產生與替換盒(S盒)相關聯之加密值之方法的流程框圖900。該方法包含獲得輸入值及第一值902，及藉由以下步驟中之一者產生S盒輸出值904：(A)對輸入值及第一值執行逐位元互斥或(XOR)操作以產生第一中間值906a，且對該第一中間值以等於該第一中間值之漢明權重的位元數目執行逐位元旋轉操作，以產生S盒輸出值908a；(B)對輸入值以等於該輸入值之漢明權重的一位元數目執行逐位元旋轉操作，以產生第一中間值906b，且對該第一中間值及第一值執行逐位元XOR操作以產生S盒輸出值908b；或(C)對輸入值及第一值執行逐位元XOR操作以產生第一中間值906c，對該第一中間值以等於該第一中間值之漢明權重的位元數目執行逐位元旋轉操作，以產生

第二中間值908c，獲得第二值910c，且對該第二中間值及該第二值執行逐位元XOR操作以產生S盒輸出值912c。

合併(一或多個)S盒之例示性電子器件

圖10說明合併本文中根據一態樣描述之S盒300、400、500、800中之任一者的電子器件1000之硬體實施的示意性方塊圖。電子器件1000可為行動電話、智慧型電話、平板電腦、攜帶型電腦，及或具有電路的任何其他電子器件。電子器件1000可包括通信介面1010、使用者介面1012，及處理系統1014。處理系統1014可包括處理電路(例如，處理器)1004、記憶體電路(例如，記憶體)1005、電腦可讀儲存媒體1006、匯流排介面1008，及匯流排1002。處理系統1014及/或處理電路1004可經組態以執行關於S盒300、400、500、800描述之步驟、函數，及/或過程中的任一者及上文關於圖3、圖4、圖5、圖6、圖7、圖8及/或圖9描述的其他電路及/或模組602、702。

處理電路1004可為經調適以處理電子器件1000之資料的一或多個處理器(例如，第一處理器等)。舉例而言，處理電路1004可為充當用於實施圖9中描述之步驟中任一者之構件的專門處理器，諸如特殊應用積體電路(ASIC)。亦即，處理電路1004可經組態以獲得輸入值及第一值，且藉由以下步驟中之一者產生S盒輸出值：(A)對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值，且對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值；(B)對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該第一中間值，且對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值；或(C)對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值，對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生一第二中間值，獲得一第

二值，且對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值。

處理電路1004之實例包括微處理器、微控制器、數位信號處理器(DSP)、場可程式化閘陣列(FPGA)、可程式化邏輯器件(PLD)、狀態機、閘控邏輯、離散硬體電路，及經組態以執行本發明通篇描述之各種功能性的其他合適硬體。處理電路1004亦負責管理匯流排1002，且執行儲存於電腦可讀儲存媒體1006及/或記憶體1005上之軟體。該軟體在藉由處理電路1004執行時導致處理電路1014執行上文關於S盒300、400、500、800描述之各種功能、步驟，及/或過程。電腦可讀儲存媒體1006可用於儲存藉由處理電路1004在執行軟體時操縱的資料。

記憶體電路1005可為非揮發性記憶體，諸如(但不限於)FLASH記憶體、磁性或光學硬碟機等等。在一些態樣中，儲存扇區資訊及/或附加項訊息(包括組態序列號)之記憶體可為可持續供電從而無限儲存資訊的揮發性記憶體，諸如DRAM(例如，DDR SDRAM)、SRAM等等。

軟體應被廣泛地解釋為意謂指令、指令集、代碼、碼段、程式碼、程式、次程式、軟體模組、應用程式、軟體應用程式、軟體套件、常式、次常式、物件、可執行碼、執行緒、程序、函數等等，而無論是被稱為軟體、韌體、中間軟體、微碼、硬體描述語言或是其他者。軟體可駐留於電腦可讀儲存媒體1006上。電腦可讀儲存媒體1006可為非暫時性電腦可讀儲存媒體。藉由實例，非暫時性電腦可讀儲存媒體包括磁性儲存器件(例如，硬碟、軟碟、磁條)、光碟(例如，緊密光碟(CD)或數位影音光碟(DVD))、智慧卡、快閃記憶體器件(例如，卡、條，或鍵驅動)、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可程式化ROM (PROM)、可抹除PROM (EPROM)、電可抹除PROM

(EEPROM)、暫存器、抽取式磁碟，及用於儲存可藉由電腦存取及讀取之軟體及/或指令的任何其他合適媒體。藉由實例，電腦可讀儲存媒體亦可包括載波、傳輸線，及用於傳輸可藉由電腦存取及讀取之軟體及/或指令的任何其他合適媒體。電腦可讀儲存媒體1006可駐留於處理系統1014中，位於處理系統1014外部，或分佈於包括處理系統1014之多個實體上。電腦可讀儲存媒體1006可體現於電腦程式產品中。

在此實例中，處理系統1014可用大體上由匯流排1002表示之匯流排架構來實施。取決於處理系統1014之特定應用及總體設計約束，匯流排1002可包括任何數目之互連匯流排及橋接器。匯流排1002將各種電路連結在一起，包括一或多個處理器(大體上由處理器1004表示)、記憶體1005，及電腦可讀媒體(大體上由電腦可讀儲存媒體1006表示)。匯流排1002亦可連結各種其他電路，諸如時序源、周邊裝置、電壓調節器及功率管理電路，該等電路係此項技術中所熟知的且因此將不再作任何進一步描述。匯流排介面1008於匯流排1002與通信介面1010(若存在)之間提供一介面。通信介面1010提供用於在傳輸媒體上與其他裝置通信的構件。取決於裝置之本質，使用者介面1012(例如，小鍵盤、顯示器、揚聲器、麥克風、觸控式螢幕顯示器等等)亦可用於電子器件1000。

圖11說明根據本發明之一態樣的處理器1004之示意性方塊圖。除其他之外，處理器1004包含一主要輸入值、輸入值、第一值，及/或第二值獲得電路1102。獲得電路1102充當用於獲得主要輸入值、輸入值、第一值，及/或第二值之構件的一實例。處理器1004進一步包含非線性變換函數電路1104，其經組態以如上文關於圖8描述的執行NLTF。

圖3、圖4、圖5、圖6、圖7、圖8、圖9、圖10，及/或圖11中所說

明之組件、步驟、特徵及/或功能的一或多者可重排及/或組合成單一組件、步驟、特徵或功能，或體現於若干組件、步驟或功能中。在不脫離本發明之情況下，亦可添加額外元件、組件、步驟及/或功能。圖3、圖4、圖5、圖6、圖7、圖8、圖10，及/或圖11中說明之裝置、器件，及/或組件可經組態以執行圖9中所描述之方法、特徵，或步驟中的一或多者。本文中描述之演算法亦可有效實施於軟體中及/或嵌入硬體中。

此外，在本發明之一態樣中，圖10及/或圖11中說明之處理電路1004可為經專門設計及/或硬連線以執行圖9中描述之演算法、方法，及/或步驟的專門處理器(例如，特殊應用積體電路(例如，ASIC))。因此，此專門處理器(例如，ASIC)可為用於執行圖9中描述之演算法、方法，及/或步驟之構件的一實例。電腦可讀儲存媒體1006亦可儲存處理器1004可讀指令，該等指令在藉由專門處理器(例如，ASIC)執行時導致該專門處理器執行圖9中描述之演算法、方法，及/或步驟。

又，應注意，可將本發明之該等態樣描述為一過程，該過程可被描繪為流程框圖、流程圖、結構圖或方塊圖。雖然流程框圖可將操作描述為順序過程，但操作中之許多者可並行或同時執行。另外，可重排該等操作之次序。當一過程之操作完成時，該過程終止。過程可對應於方法、函數、程序、次常式、次程式等。當一過程對應於函數時，其終止對應於該函數返回至調用函數或主函數。

此外，儲存媒體可表示用於儲存資料之一或多個器件，包括唯讀記憶體(ROM)、隨機存取記憶體(RAM)、磁碟儲存媒體、光學儲存媒體、快閃記憶體器件及/或用於儲存資訊之其他機器可讀媒體及處理器可讀媒體，及/或電腦可讀媒體。術語「機器可讀媒體」、「電腦可讀媒體」，及/或「處理器可讀媒體」可包括(但不限於)非暫時性媒體，諸如攜帶型或固定型儲存器件、光學儲存器件，及能夠儲存、包

含，或載運指令及/或資料之各種其他媒體。因此，本文中描述之各種方法可藉由可儲存於「機器可讀媒體」、「電腦可讀媒體」，及/或「處理器可讀媒體」中且藉由一或多個處理器、機器，及/或器件執行的指令及/或資料完全或部分實施。

另外，本發明之態樣可由硬體、軟體、韌體、中間軟體、微碼、或其任一組合來實施。當實施於軟體、韌體、中間軟體或微碼中時，可將用以執行必要任務之程式碼或碼段儲存於諸如儲存媒體或其他儲存器之機器可讀媒體中。處理器可執行必要任務。碼段可表示程序、函數、次程式、程式、常式、次常式、模組、軟體套件、類別、或指令、資料結構或程式敘述的任一組合。可藉由傳遞及/或接收資訊、資料、引數、參數或記憶體內容而將一碼段耦接至另一碼段或硬體電路。可經由包括記憶體共用、訊息傳遞、符記傳遞、網路傳輸等等之任何合適方式來傳遞、轉發或傳輸資訊、引數、參數、資料等等。

結合本文中所揭示之實例而描述之各種說明性邏輯區塊、模組、電路、元件及/或組件可以通用處理器、數位信號處理器(DSP)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)或其他可程式化邏輯組件、離散閘或電晶體邏輯、離散硬體組件或其經設計以執行本文中所描述之功能之任何組合來實施或執行。通用處理器可為微處理器，但在替代例中，處理器可為任何習知之處理器、控制器、微控制器或狀態機。處理器亦可被實施為計算組件之組合，例如，DSP與微處理器之組合、許多微處理器、結合DSP核心之一或多個微處理器，或任何其他此種組態。

結合本文中揭示之實例所描述之方法及演算法可以處理單元、程式化指令或其他指導之形式直接體現於硬體、可由處理器執行之軟體模組或兩者之組合中，且可含於單一器件中或分佈於多個器件上。

軟體模組可駐留於RAM記憶體、快閃記憶體、ROM記憶體、EPROM記憶體、EEPROM記憶體、暫存器、硬碟、抽取式磁碟、CD-ROM、或此項技術中已知的任一其他形式之儲存媒體中。儲存媒體可耦接至處理器，使得該處理器可自該儲存媒體讀取資訊，並可將資訊寫入至該儲存媒體。在替代例中，儲存媒體可整合至處理器。

熟習此項技術者將進一步瞭解，結合本文中所揭示之態樣而描述的各種說明性邏輯區塊、模組、電路及演算法步驟可實施為電子硬體、電腦軟體或兩者之組合。為了清楚地說明硬體與軟體之此可互換性，上文已大體上在功能性方面描述了各種說明性組件、區塊、模組、電路及步驟。此功能性經實施為硬體或是軟體取決於特定應用及強加於整個系統之設計約束而定。

本文中所描述之本發明之各種特徵可在不脫離本發明之情況下實施於不同系統中。應注意，揭示內容之前述態樣僅為實例，且不應理解為限制本發明。本揭示內容之態樣的描述意圖為說明性的，且不限制申請專利範圍之範疇。因此，本發明之教示可易於應用於其他類型之裝置，且許多替代、修改及變化對於彼等熟習此項技術者而言將為顯而易見的。

【符號說明】

100	S盒
102	旋轉函數
200	表
300	替換盒(S盒)
302	逐位元互斥或(XOR)函數
304	旋轉函數
400	S盒
402	旋轉函數

404	逐位元XOR函數
500	S盒
502	逐位元XOR函數
504	旋轉函數
506	逐位元XOR函數
602	加密函數
702	密碼模組/密碼區塊
704	組件
706	組件
708	組件
800	S盒
802	位元分配電路
803a-n	NLTF輸入值
804	非線性變換函數(NLTF)子電路
805a-n	NLTF輸出值
806	非線性變換函數(NLTF)子電路
808	非線性變換函數(NLTF)子電路
810	非線性變換函數(NLTF)子電路
812	串接電路
814	S盒A子電路/S盒子電路A
900	流程框圖
1000	電子器件
1002	匯流排
1004	處理電路/處理器
1005	記憶體電路
1006	電腦可讀儲存媒體

1008	匯流排介面
1010	通信介面
1012	使用者介面
1014	處理系統
1102	主要輸入值、輸入值、第一值，及/或第二值獲得電路
1104	非線性變換函數電路
C_1	變值
C_2	變值
f	加密函數
K_1	金鑰/識別符
w	第一中間輸出/第一中間值
W	HWBF之輸出
x	輸入
y	第一中間輸出/第二中間輸出/第二中間值/n位元輸入值
z	輸出

申請專利範圍

1. 一種用於產生與一替換盒(S盒)相關聯之加密值的方法，該方法包含：

獲得一輸入值及一第一值；及

藉由以下步驟中之一者產生一S盒輸出值：

(A) 對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值，且

對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值；

(B) 對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該第一中間值，且

對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值；或

(C) 對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值，

對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生一第二中間值，

獲得一第二值，且

對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值。

2. 如請求項1之方法，其中所提供之該第一值及/或該第二值中的至少一者經組態以產生具有等於或大於50%可能性之與該輸入值具有一不同漢明權重的該S盒輸出值。

3. 如請求項1之方法，其中該第一值及/或該第二值中的至少一者為具有一非零漢明權重的一常數。

4. 如請求項1之方法，其中所提供之該第一值及/或該第二值中的至少一者係可變的，且具有等於或大於百分之100*(1 - 2^{-n})的具有一非零漢明權重之一可能性，其中n為該第一值及/或該第二值之一位元數目。

5. 如請求項1之方法，其中該第一值及/或該第二值中的至少一者係自一加密函數及/或加密金鑰中的至少一者導出。

6. 如請求項1之方法，其中該第一值及/或該第二值中的至少一者係自一加密模組的一組件級導出。

7. 如請求項6之方法，其中該密碼模組為一流密碼。

8. 如請求項1之方法，其中該方法於一記憶體電路中執行。

9. 如請求項1之方法，其中該輸入值及該S盒輸出值具有相同位元數目。

10. 如請求項1之方法，其進一步包含：

獲得一主要輸入值；

分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；

將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及

串接該複數個NLTF輸出值以獲得該輸入值。

11. 如請求項10之方法，其中該主要輸入值經分配使得該複數個NLTF輸入值中之每一者具有相同位元數目。

12. 一種電子器件，其包含：

一處理電路，其經組態以

獲得一輸入值及一第一值；及

藉由以下步驟中之一者產生一替換盒(S盒)輸出值：

(A) 對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值，且

對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值；

(B) 對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該第一中間值，且

對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值；或

(C) 對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值，

對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生一第二中間值，

獲得一第二值，且

對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值。

13. 如請求項12之電子器件，其中所提供之該第一值及/或該第二值中的至少一者經組態以產生具有等於或大於50%可能性之與該輸入值具有一不同漢明權重的該S盒輸出值。

14. 如請求項12之電子器件，其中該第一值及/或該第二值中的至少一者為具有一非零漢明權重的一常數。

15. 如請求項12之電子器件，其中所提供之該第一值及/或該第二值中的至少一者係可變的，且具有等於或大於百分之$100*(1 - 2^{-n})$的具有一非零漢明權重之一可能性，其中n為該第一值及/或該第二值之一位元數目。

16. 如請求項12之電子器件，其中該第一值及/或該第二值中的至少

一者係自一加密函數及/或加密金鑰中的至少一者導出。

17. 如請求項12之電子器件，其中該第一值及/或該第二值中的至少一者係自一加密模組的一組件級導出。

18. 如請求項12之電子器件，其中該處理電路經進一步組態以：

獲得一主要輸入值；

分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；

將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及

串接該複數個NLTF輸出值以獲得該輸入值。

19. 一種電子器件，其包含：

用於獲得一輸入值及一第一值的構件；及

用於藉由以下步驟中之一者產生一替換盒(S盒)輸出值的構件：

(A) 用於對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值的構件，及

用於對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值的構件；

(B) 用於對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該第一中間值的構件，及

用於對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值的構件；或

(C) 用於對該輸入值及該第一值執行一逐位元XOR操作以產

生該第一中間值的構件，

用於對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生一第二中間值的構件，

用於獲得一第二值的構件，及

用於對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值的構件。

20. 如請求項19之電子器件，其中所提供之該第一值及/或該第二值中的至少一者經組態以產生具有等於或大於50%可能性之與該輸入值具有一不同漢明權重的該S盒輸出值。

21. 如請求項19之電子器件，其中該第一值及/或該第二值中的至少一者為具有一非零漢明權重的一常數。

22. 如請求項19之電子器件，其中該第一值及/或該第二值中的至少一者係自一加密函數及/或加密金鑰中的至少一者導出。

23. 如請求項19之電子器件，其中該第一值及/或該第二值中的至少一者係自一加密模組的一組件級導出。

24. 如請求項19之電子器件，其進一步包含：

用於獲得一主要輸入值的構件；

用於分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值的構件，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；

用於將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值的構件，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及

用於串接該複數個NLTF輸出值以獲得該輸入值的構件。

25. 一種電腦可讀儲存媒體，其具有儲存於其上之用於產生與一替

換盒(S盒)相關聯之加密值的指令，該指令在藉由至少一處理器執行時使得該處理器：

獲得一輸入值及一第一值；及

藉由以下步驟中之一者產生一S盒輸出值：

(A) 對該輸入值及該第一值執行一逐位元互斥或(XOR)操作以產生一第一中間值，且

對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該S盒輸出值；

(B) 對該輸入值以等於該輸入值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生該第一中間值，且

對該第一中間值及該第一值執行一逐位元XOR操作以產生該S盒輸出值；或

(C) 對該輸入值及該第一值執行一逐位元XOR操作以產生該第一中間值，

對該第一中間值以等於該第一中間值之漢明權重的一位元數目執行一逐位元旋轉操作，以產生一第二中間值，

獲得一第二值，且

對該第二中間值及該第二值執行一逐位元XOR操作以產生該S盒輸出值。

26. 如請求項25之電腦可讀儲存媒體，其中所提供之該第一值及/或該第二值中的至少一者經組態以產生具有等於或大於50%可能性之與該輸入值具有一不同漢明權重的該S盒輸出值。

27. 如請求項25之電腦可讀儲存媒體，其中該第一值及/或該第二值中的至少一者為具有一非零漢明權重的一常數。

28. 如請求項25之電腦可讀儲存媒體，其中該等指令在藉由該處理器執行時進一步使得該處理器：

獲得一主要輸入值；

分配該主要輸入值之位元以獲得複數個非線性變換函數(NLTF)輸入值，其中每一NLTF輸入值具有小於該主要輸入值之一位元數目的一位元數目；

將該等NLTF輸入值中之每一者提供至執行一非線性操作的一NLTF以產生複數個NLTF輸出值，該複數個NLTF輸出值的每一者對應於提供至該NLTF之該NLTF輸入值；及

串接該複數個NLTF輸出值以獲得該輸入值。

圖式

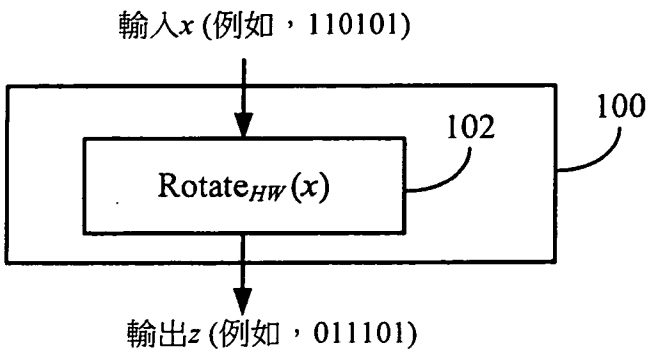

圖1

輸出z 位元	值	**HWBF**
LSB	1	$W(x)$
第二**LSB**	0	$W(x<<1)$
第三**LSB**	1	$W(x<<2)$
第四**LSB**	1	$W(x<<3)$
第五**LSB**	1	$W(x<<4)$
第六**LSB**	0	$W(x<<5)$

200

圖2

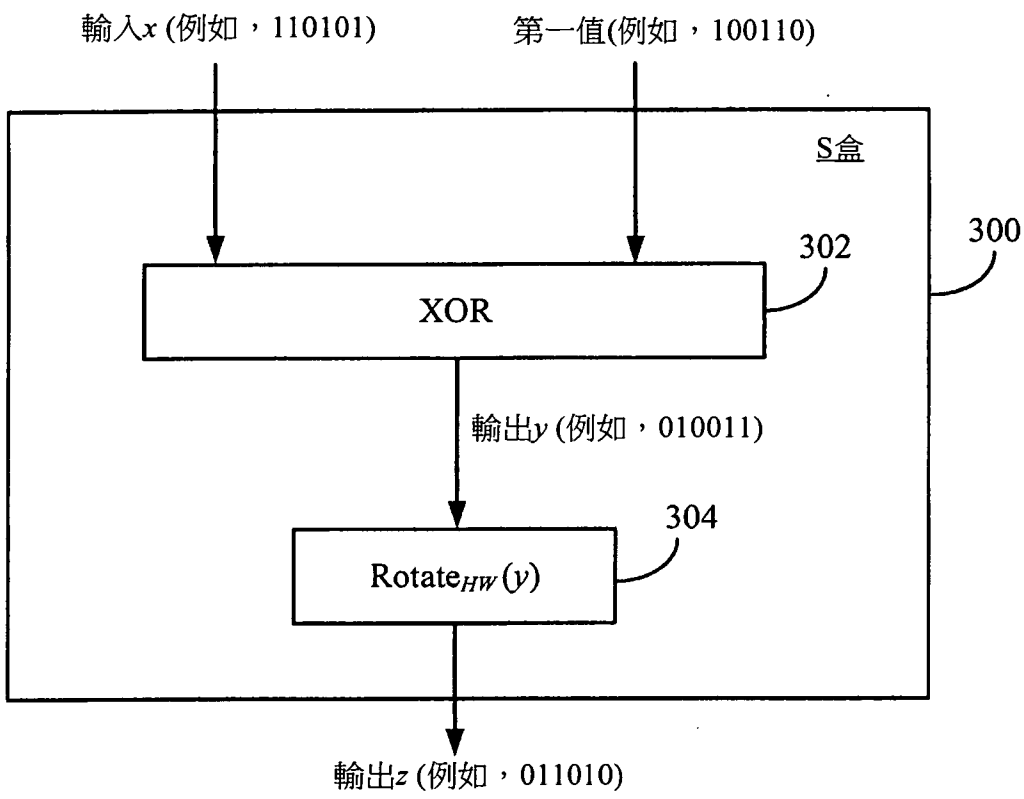
輸入x (例如，110101)
第一值(例如，100110)
S盒
300
302
XOR
輸出y (例如，010011)
304
Rotate$_{HW}$(y)
輸出z (例如，011010)

圖3

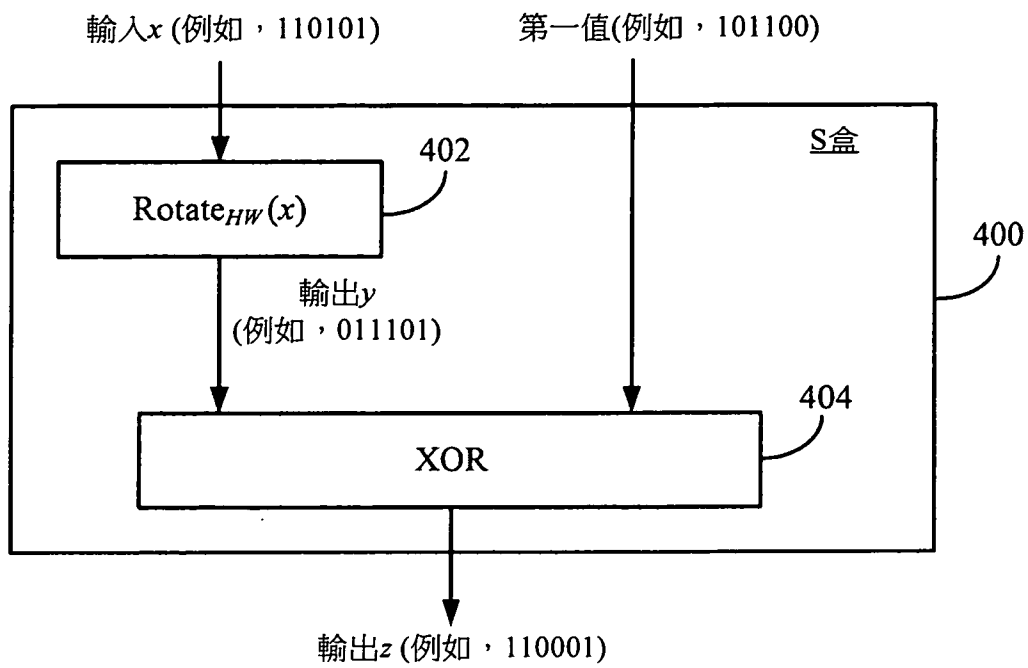
輸入x (例如，110101)
第一值(例如，101100)
S盒
402
Rotate$_{HW}$(x)
400
輸出y
(例如，011101)
404
XOR
輸出z (例如，110001)

圖4

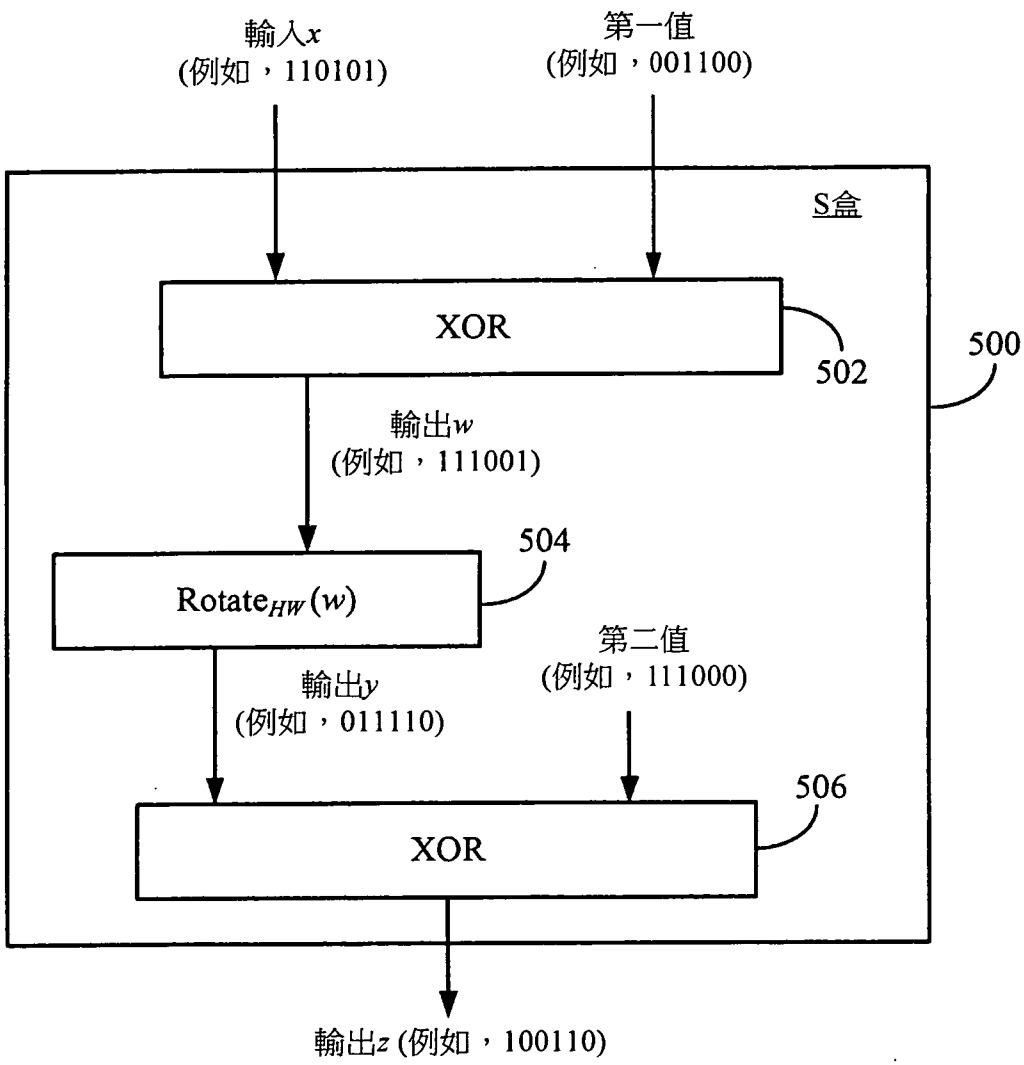
輸入x
(例如，110101)
第一值
(例如，001100)
S盒
XOR
502
500
輸出w
(例如，111001)
504
Rotate$_{HW}$(w)
第二值
(例如，111000)
輸出y
(例如，011110)
506
XOR
輸出z (例如，100110)

圖5

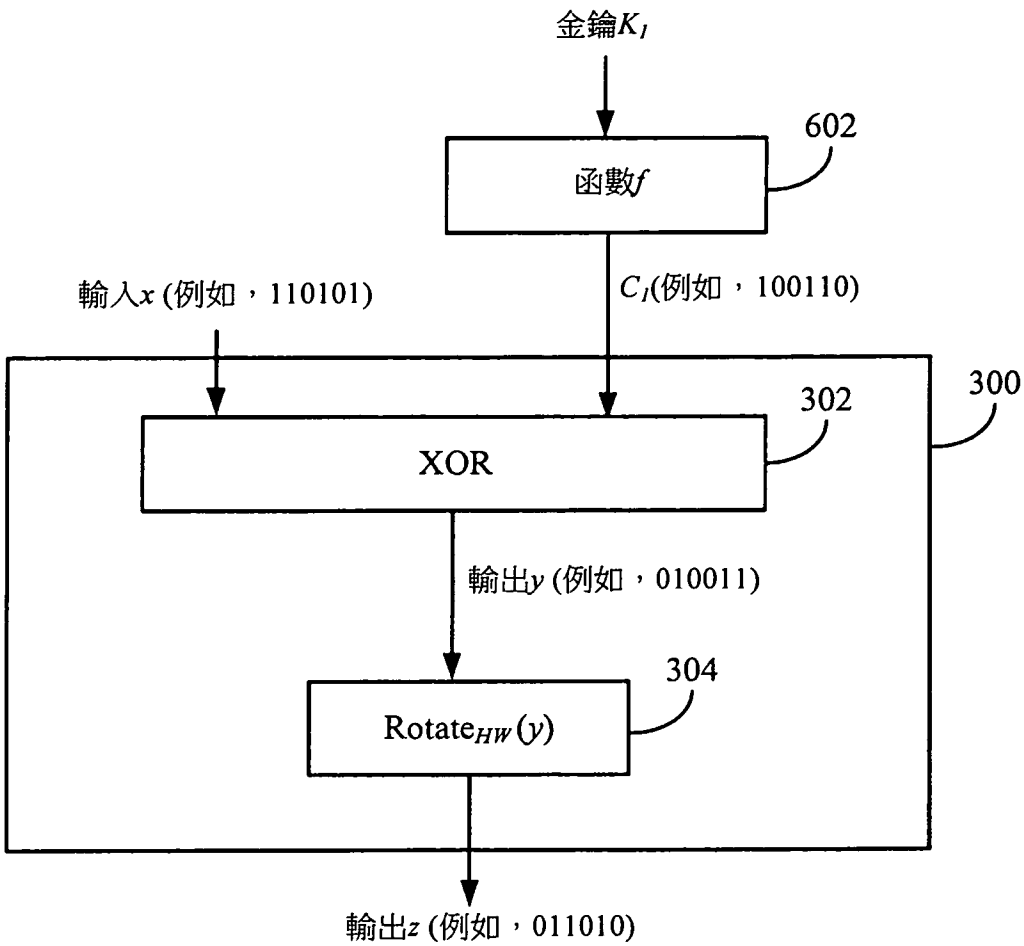
金鑰K_I
602
函數f
輸入x (例如，110101)
C_I(例如，100110)
300
302
XOR
輸出y (例如，010011)
304
Rotate$_{HW}$(y)
輸出z (例如，011010)

圖6

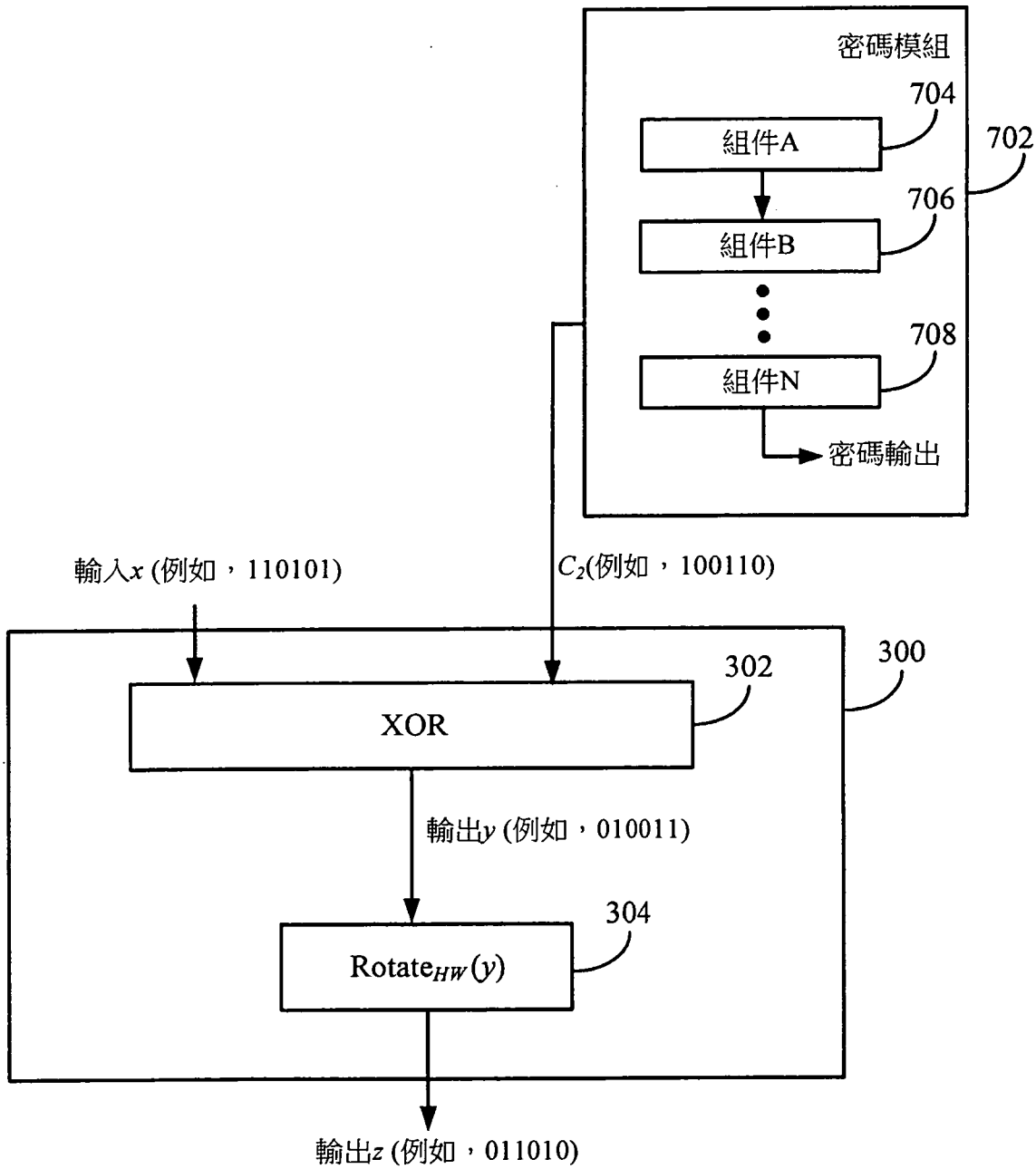
密碼模組
704
組件A
702
706
組件B
708
組件N
密碼輸出
輸入x (例如，110101)
C2(例如，100110)
300
302
XOR
輸出y (例如，010011)
304
Rotate_HW(y)
輸出z (例如，011010)

圖7

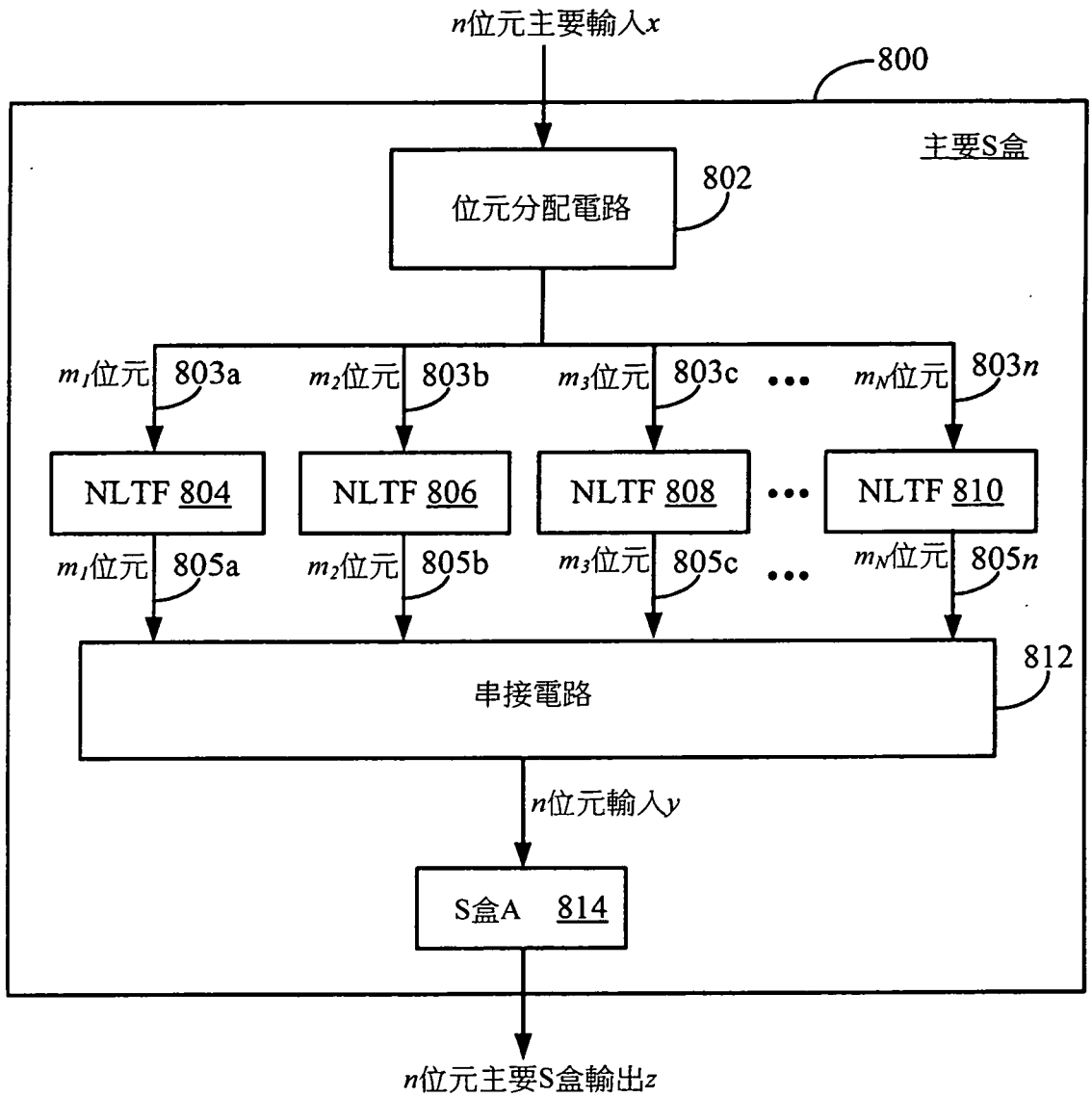
n位元主要輸入x
800
主要S盒
位元分配電路
802
m1位元
803a
m2位元
803b
m3位元
803c
mN位元
803n
NLTF 804
NLTF 806
NLTF 808
NLTF 810
m1位元
805a
m2位元
805b
m3位元
805c
mN位元
805n
串接電路
812
n位元輸入y
S盒A 814
n位元主要S盒輸出z

圖8

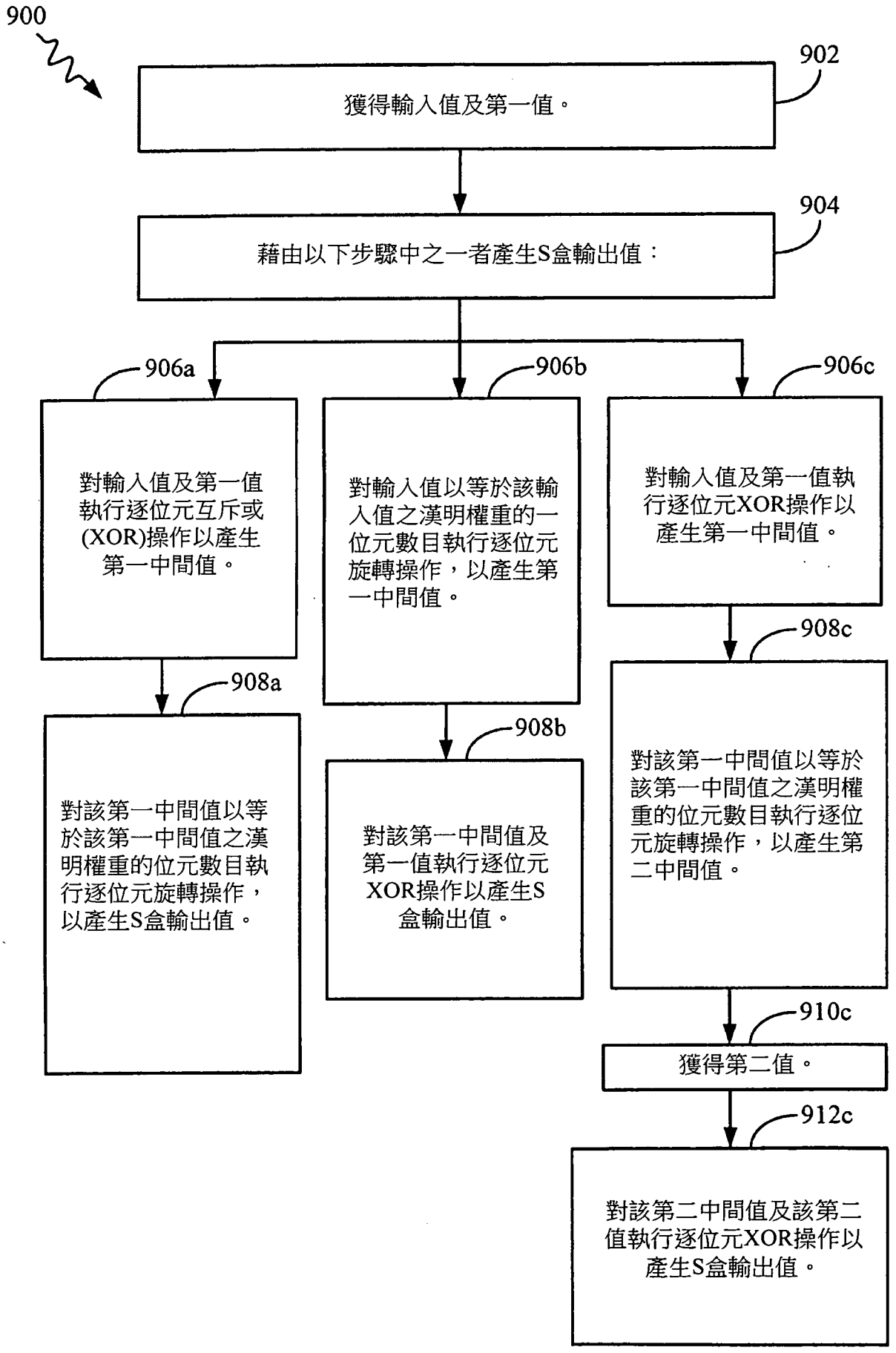
900
902
獲得輸入值及第一值。
904
藉由以下步驟中之一者產生S盒輸出值：
906a
對輸入值及第一值執行逐位元互斥或(XOR)操作以產生第一中間值。
906b
對輸入值以等於該輸入值之漢明權重的一位元數目執行逐位元旋轉操作，以產生第一中間值。
906c
對輸入值及第一值執行逐位元XOR操作以產生第一中間值。
908a
對該第一中間值以等於該第一中間值之漢明權重的位元數目執行逐位元旋轉操作，以產生S盒輸出值。
908b
對該第一中間值及第一值執行逐位元XOR操作以產生S盒輸出值。
908c
對該第一中間值以等於該第一中間值之漢明權重的位元數目執行逐位元旋轉操作，以產生第二中間值。
910c
獲得第二值。
912c
對該第二中間值及該第二值執行逐位元XOR操作以產生S盒輸出值。

圖9

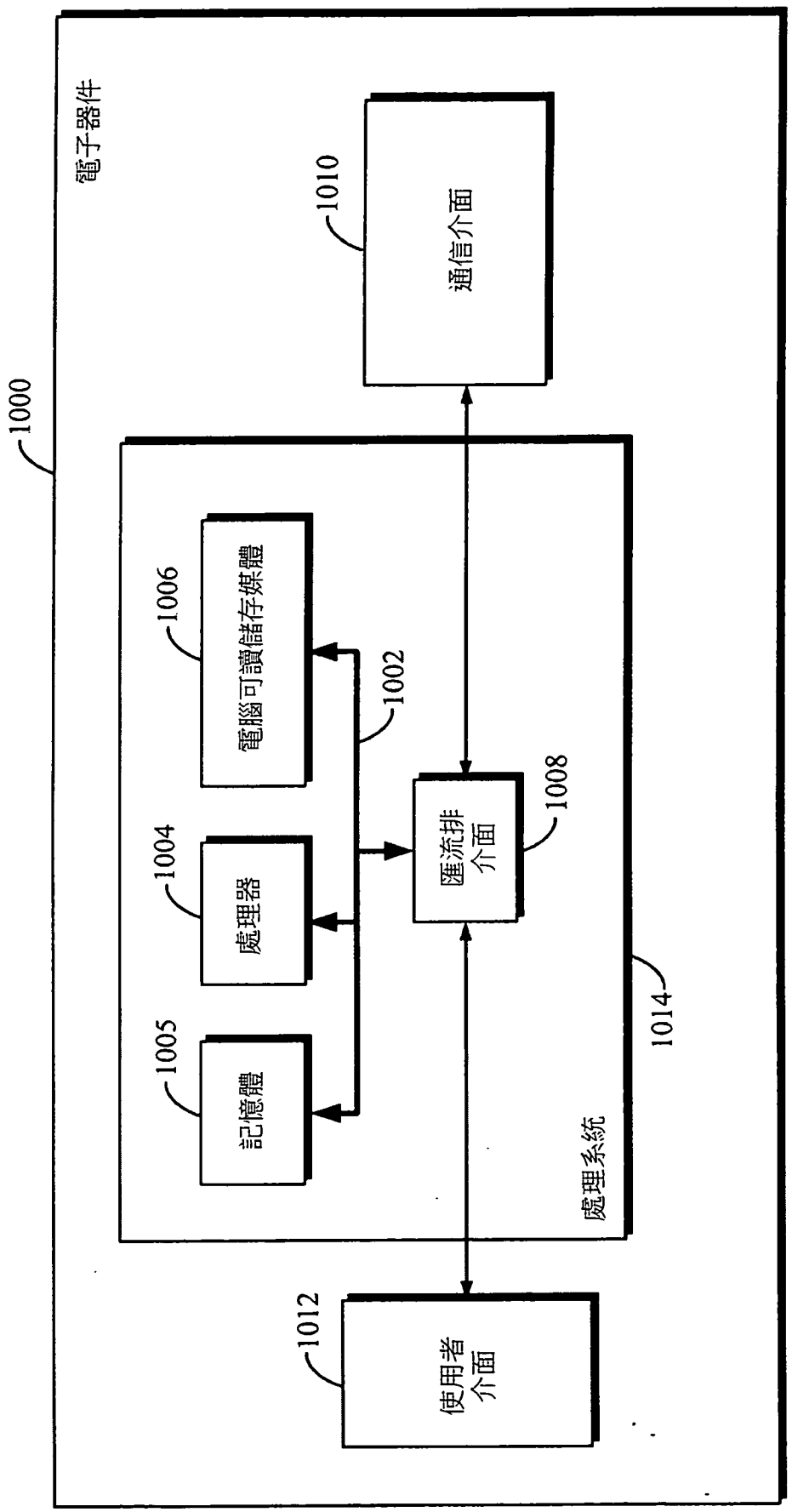
電子器件
1000
1010
通信介面
1006
電腦可讀儲存媒體
1002
1004
處理器
1008
匯流排介面
1005
記憶體
1014
處理系統
1012
使用者介面

圖10

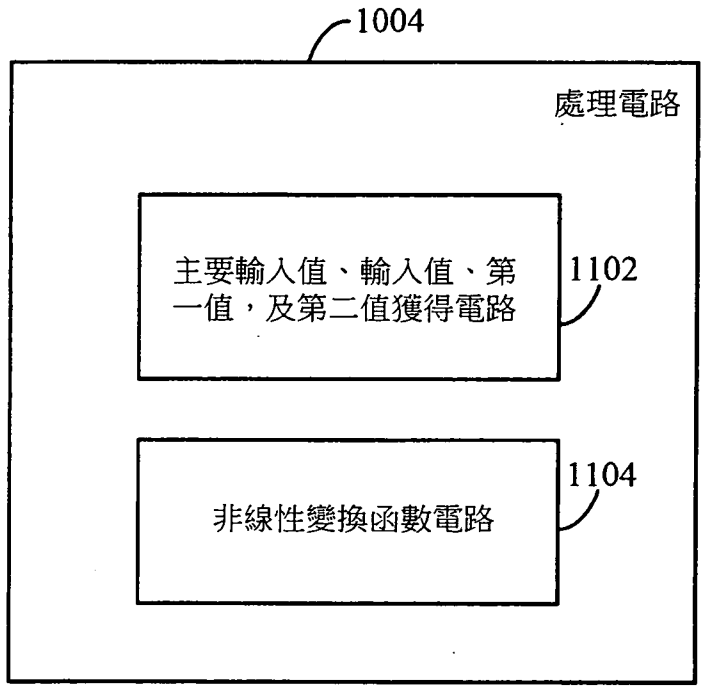

圖11