

公告本

發明專利說明書

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：97150722

※申請日期：97.12.25

※IPC 分類：

H04L 9/22

(2006.01)

一、發明名稱：(中文/英文)

安全隨機號碼產生器

SECURE RANDOM NUMBER GENERATOR

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

美商艾基爾系統公司

AGERE SYSTEMS INC.

代表人：(中文/英文)

大衛 L 史密斯

SMITH, DAVID L.

住居所或營業所地址：(中文/英文)

美國賓州亞倫鎮市美國公園東北路1110號

1110 AMERICAN PARKWAY NE, ALLENTOWN, PENNSYLVANIA

18109, U.S.A.

國籍：(中文/英文)

美國 U.S.A.

三、發明人：(共 5 人)

姓 名：(中文/英文)

1. 艾德華 B 哈利斯
HARRIS, EDWARD B.
2. 理查 侯格
HOGG, RICHARD
3. 羅斯 A 寇樂
KOHLER, ROSS A.
4. 理查 J 麥帕藍
MCPARTLAND, RICHARD J.
5. 威恩 E 偉爾諾
WERNER, WAYNE E.

國 籍：(中文/英文)

1. 美國 U.S.A.
2. 美國 U.S.A.
3. 美國 U.S.A.
4. 美國 U.S.A.
5. 美國 U.S.A.

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 世界智慧財產權組織；2008年05月23日；PCT/US08/64679
- 2.

☐ 無主張專利法第二十七條第一項國際優先權：

- 1.
- 2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

本發明揭示一種隨機號碼產生器電路，其包含一具有複數個儲存元件的第一記憶體。當被一施加至該第一記憶體的電壓供應源供電時，該等儲存元件之每一者具有一與其相應的初始狀態。該第一記憶體可操作以產生一第一信號，該第一信號包含複數個指示該等儲存元件之各自初始狀態的位元。該隨機號碼產生器電路進一步包含一耦合至該第一記憶體的錯誤校正電路。該錯誤校正電路可操作以接收該第一信號及校正該第一信號中至少一個不會基於電力對該第一記憶體之連續施加而重複的位元以便藉此產生一第二信號。該第二信號係一個可基於電力對該第一記憶體之連續施加而重複的隨機號碼。

六、英文發明摘要：

A random number generator circuit includes a first memory having multiple storage elements. Each of the storage elements has an initial state corresponding thereto when powered up by a voltage supply source applied to the first memory. The first memory is operative to generate a first signal including multiple bits indicative of the respective initial states of the storage elements. The random number generator circuit further includes an error correction circuit coupled to the first memory. The error correction circuit is operative to receive the first signal and to correct at least one bit in the first signal that is not repeatable upon successive applications of power to the first memory to thereby generate a second signal. The second signal is a random number that is repeatable upon successive applications of power to the first memory.

七、指定代表圖：

(一)本案指定代表圖為：第 (2) 圖。

(二)本代表圖之元件符號簡單說明：

201	記憶體
202	電源
203	錯誤校正電路
204	錯誤碼記憶體
205	控制器
206	未校正隨機號碼
207	校正隨機號碼
208	錯誤校正碼

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

九、發明說明：

【發明所屬之技術領域】

本發明大體上係關於電氣、電子及電腦技術，更具體而言係關於隨機號碼的產生。

【先前技術】

在一些包含但不限於電子商務(e商務)、可攜式通信裝置(例如行動電話)、固態媒體儲存裝置等的應用中，需要安全碼以保護被儲存之資料及/或裝置之使用。安全碼，或其所演算而來的代碼或號碼，一般被儲存於內嵌於積體電路(IC)晶片中的非揮發性記憶體中，例如快閃記憶體及一次性可編程(OTP)記憶體中。非揮發性記憶體被用於確保當晶片被切斷電源時該等安全碼被留駐於該主晶片中。為提供一種安全環境，必要的係安全碼不會被習知的觀測或逆向工程方法檢測。但不幸的係在內嵌非揮發性記憶體中儲存安全碼的多數習知方法可經由視覺檢查、掃描電子顯微鏡(SEM)影像及/或電荷測量技術檢測。

舉例來說，內嵌快閃記憶體係可用獨特安全碼變成的非揮發性記憶體。然而，快閃記憶體單元之編程資料狀態可藉由習知的電荷測量方法而被確定。包含氧化物擊穿反熔絲記憶體及金屬或多晶矽(多)熔絲記憶體的OTP記憶體可用獨特安全碼編程且係非揮發性的。然而，該等記憶體單元之變成資料狀態可使用SEM或替代影像技術藉由該反熔絲記憶體中之閘極氧化物擊穿區域之檢查而被確定。與之相似的係在一金屬或多晶矽熔絲記憶體中該等分別的單元

之編程資料狀態可藉由層移除及視覺檢查而被確定。因此，用於將安全碼編程至非揮發性記憶體中的習知方法缺少足夠的安全保證，因此係不理想的。

作為對將安全碼編程至非揮發性記憶體中的替代，安全碼可被產生於該主晶片(例如至少部分地基於代碼或隨機號碼產生器)之外，傳送至該晶片然後被儲存在內嵌於該晶片的非揮發性記憶體中。其不理想之處在於其易受盜竊的影響，這主要係因為已知的係該等安全碼在該主晶片環境之外，且因此可被攔截及/或操縱。

因此，存在一種對於確保儲存資料及/或裝置使用之安全且沒有習知技術所具有之該等限制之技術的需求。

【發明內容】

本發明之實施例藉由提供用於安全隨機號碼之產生的技術而滿足上述需求。經由在一晶片中隨機號碼的可重複產生，利用習知的觀測及/或逆向工程方法發現這些隨機安全號碼不可能，本發明之技術為安全碼提供實際上防盜的、非揮發性記憶體儲存。

根據本發明之一態樣，一種隨機號碼產生器電路被提供。該隨機號碼產生器電路包含一具有複數個儲存元件的第一記憶體。當被一施加至該第一記憶體的電壓電源供電時，該等儲存元件之每一者具有一與其相應的初始狀態。該第一記憶體可操作以產生一第一信號，該第一信號包含複數個指示該等儲存元件之各自初始狀態的位元。該隨機號碼產生器進一步包含一耦合至該第一記憶體的錯誤校正

電路。該錯誤校正電路可操作以接收該第一信號及校正該第一信號中至少一個不會基於電力對該第一記憶體之連續施加而重複的位元以便藉此產生一第二信號。該第二信號係一個可基於電力對該第一記憶體之連續施加而重複的隨機號碼。一或多個隨機號碼產生器電路可被包含於一積體電路中。

根據本發明之另一態樣，一種產生一安全隨機號碼的方法包含如下步驟：對一包括複數個儲存元件的第一記憶體供電，當被供電時各個該等儲存元件具有一與其相應的初始狀態；產生一第一信號，該第一信號包括複數個指示該等儲存元件之分別初始狀態的位元；及校正該第一信號中的非可重複位元藉以產生一第二信號，該第二信號係一個可基於電力對該第一記憶體之連續施加而重複的隨機號碼。

根據本發明之另一態樣，一電子系統包含至少一個積體電路，該積體電路包含至少一個隨機號碼產生器電路。該隨機號碼產生器電路包括一第一記憶體，該第一記憶體包含複數個儲存元件。當被一施加至該第一記憶體的電壓電源供電時，該等儲存元件之每一者具有一與其相應的初始狀態。該第一記憶體可操作以產生一第一信號，該第一信號包含複數個指示該等儲存元件之各自初始狀態的位元。該隨機號碼產生器進一步包含一耦合至該第一記憶體的錯誤校正電路。該錯誤校正電路可操作以接收該第一信號並校正該第一信號中的非可重複位元藉以產生一第二信號作

為該隨機號碼產生器電路之一輸出。該第二信號係一個可基於電力對該第一記憶體之連續施加而重複的隨機號碼。一或多個隨機號碼產生器電路可被包含於一積體電路中。

本發明之這些及其它特徵、目的及優點將基於其說明性實施例的如下詳細描述而變得明顯，該描述將結合該等圖式來閱讀。

【實施方式】

本發明將以一示例性記憶體電路、隨機號碼產生器電路及隨機號碼產生方法的內容來予以描述。然而，應理解本發明之技術不限於顯示及描述於此的該等電路及方法。本發明之實施例係廣泛地針對用於確保儲存資料及/或裝置使用之安全的技術。經由在一晶片中隨機號碼的可重複產生，利用習知的觀測及/或逆向工程方法發現這些隨機安全號碼不可能，說明性實施例為安全碼提供實際上防盜的、非揮發性記憶體儲存。雖然本發明之較佳實施例可被製造於一矽晶圓中，本發明之實施例亦可替代地被製造於包括其他材料的晶圓中，這些其他材料包含但不限於砷化鎵(GaAs)、磷化銦(InP)等。

圖1為一可結合本發明之一實施例而使用的示例性SRAM陣列18之一概要圖。SRAM陣列18包含複數個配置於一N列及M行之陣列中的SRAM單元20，一單元駐留於一列及一行的各個相交處，其中N及M為整數。相應於SRAM陣列18中之一規定列的SRAM單元20較佳地被連接至一共用列線(例如列0或列N)，其亦被稱為一字線。與之相似的係

相應於一規定行的SRAM單元20較佳地被連接至一對互補共用行線(例如行0及行C0或行M及行CM)，其亦被稱為位元線。在每對行線中，行C代表行之一邏輯補充。

較佳的係各個SRAM單元20為一六電晶體單元，包括兩個n通道金屬氧化物半導體(NMOS)下拉電晶體裝置40及42、兩個p通道金屬氧化物半導體(PMOS)上拉電晶體裝置46及48、以及兩個NMOS存取電晶體裝置30及32。本發明不限於被顯示的該具體記憶體單元組態。更詳細而言，裝置46及48之源極被彼此連接並適於連接至一第一電壓源，其可為VDD；裝置46之一汲極被在節點34處連接至裝置40之汲極；裝置40及42之源極被彼此連接並適於連接至一第二電壓源，其可為地線；裝置42之一汲極在節點36處連接至裝置48之一汲極；裝置46及40之閘極在節點36處連接至裝置48及42之汲極。裝置48及42之閘極在節點34處連接至裝置46及40之汲極。存取電晶體30之一汲極被連接至節點34；存取裝置32之一汲極被連接至節點36；裝置30之一源極適於連接至一相應的行線(例如行0)；裝置32之一源極適於連接至一相應的互補行線(例如行C0)；及裝置30、32之閘極被連接至一相應的列線(例如列0)。

SRAM單元20可被配置於一如圖1所示的陣列中。對於配置於一N列及M行之陣列中的記憶體單元來說，典型的係需要至少N個記憶體讀取週期以讀取所有單元。或者SRAM單元20可被配置於一單一系列(未顯示)中，在此情況下該等單元可被於一單一記憶體讀取週期中存取。此外，

較佳的係該等行線被定向於一大體垂直的維度中，而該等列線被定向於一大體水平的維度中，使得該等列及行線大體彼此成直角。然而，應理解本發明不限於任何具體的記憶體單元配置及/或列及行線定向。舉例來說，該等列及行線的其他定向(例如成斜角)亦可被考慮且被包含於本發明之範圍中。

當首次被供電時，一代表性記憶體單元可處於兩個穩定初始狀態中的一個狀態下，即一指示一可為VDD(例如大約3.3伏特)之邏輯高位準的第一狀態(例如二進位數字「1」)，或一指示一可為零伏特之邏輯低位準的第二狀態(例如二進位數字「0」)。使用於此之術語初始狀態旨在被界定為該記憶體單元在被供電之後及被寫入之間的資料狀態。理想的係一SRAM單元被設計為一對稱並平衡的電路，因此當被供電時該SRAM單元具有一處於二進位數字1或二進位數字0之一初始狀態下的均等機率。一規定記憶體單元之初始狀態主要被製程差異及波動決定。與任何物理結構一樣，典型的係差異存在於尺寸、組分含量及其它物理屬性中。

具體而言，在大多數類型的記憶體單元之情況下，尤其係在SRAM記憶體單元中，某些與形成一規定記憶體單元之電晶體關聯之特性中的差異可產生，包含，例如，電晶體源極及汲極區域內的摻雜位準、一電晶體通道區域內的摻雜位準、電晶體閘極氧化物電容、電晶體閘極氧化物中的捕獲電荷、電晶體通道區域中的捕獲電荷、電晶體區域

之間的幾何偏移、電晶體通道長度及電晶體通道寬度...等。此外，差異可產生於例如互連厚度、長度及寬度、記憶體單元之電阻及電容中。這些物理方面及/或與該等記憶體單元相關之製程參數中的差異主要係隨機的，因此，對於各個記憶體單元來說，在被供電後在該單元中達到的二進位狀態基本上係隨機的。

應理解，適用於本發明之該等記憶體單元可包括任何具有被非編程處理及/或尺寸差異所設置之初始狀態的電路元件。如此之記憶體單元可包含，但不限於，正反器、鎖存器、顯示於圖1中的該說明性SRAM單元類型、其他SRAM單元類型、其他互補金屬氧化物半導體(CMOS)電路元件等。

由於在製程及/或與該等單元關聯之尺寸特性中的差異，在一記憶體陣列中多數SRAM單元具有一足夠大的合成失衡以引起一可重複初始狀態，之後其將稱為一明確初始狀態。在此情況下，每次當一記憶體單元被供電時，其初始狀態將總是相同；總是為一二進位數字0或總是為一二進位數字1狀態。然而，在一記憶體陣列中存在幾近電平衡之記憶體單元之某個子集，雖然該子集較小-這些單元未能在該相同狀態下始終如一地供電。在此情況下，不存在足夠的淨失衡以引起一明確初始狀態。展現一之後可被引用為一明確初始狀態的不會重複初始狀態之記憶體單元可被其他隨時間變化的差異例如，但不限於，晶片溫度、電源電壓位準、電源電壓轉換速率及該單元附近的電雜訊

(例如切換雜訊、串擾等)影響。

由於製程差異基本上係隨機的，因此一規定記憶體單元之該可重複初始狀態係已知的。如此之初始狀態雖可重複，但具有處於一二進位數字1或0之狀態的大約均等的幾率。因此，一源自一些記憶體單元之初始狀態的安全碼將為一隨機號碼。在一記憶體陣列中，具有明確初始狀態的記憶體單元提供該記憶體陣列之一可重複簽名。然而，如前所述，在該記憶體陣列中可能存在不展現可重複初始狀態之記憶體單元的一個較小子集。在如此之情況下，每次該晶片被供電時，從該記憶體陣列產生之最終隨機號碼將非為一致的。對於安全碼之產生來說，理想的係每次該晶片供電時都具有相同的隨機號碼。因此，為產生一可重複隨機號碼，具有一明確初始狀態的記憶體單元必須以某種方式被定址。

根據本發明之一態樣，錯誤校正技術可被有利地利用以界定具有明確初始狀態的記憶體單元之狀態。總體而言，錯誤校正碼(ECC)可被用於校正從一記憶體讀取的資料。一個較簡單的ECC形式係基於分組碼。一種被廣泛使用的分組碼係漢明碼。裏德-所羅門(Reed-Soloman；RS)碼及博斯-喬赫裏-霍克文黑姆(Bose-Chaudhuri-Hocquenghem；BCH)碼係其他習知的錯誤校正碼。錯誤校正之方法被習知於技術中(見例如Roberto Togneri及Christopher J.S. deSilva所著之《資訊理論及編碼設計原理》，Chapman & Hall/CRC出版社，2002年)。因此，為了簡潔說明，錯誤校正理論之

一詳細討論將不被呈現於此。本發明之技術可被用於基於一IC的供電而產生一隨機、可靠且可重複的安全碼。此外，作為由IC製程及/或尺寸差異引起的淨記憶體單元失衡之一功能而產生的該安全碼不能經由習知的檢查及/或逆向工程方法而被合理確定。

圖2為一根據本發明之一實施例的示例性隨機號碼產生器電路200之一方塊圖。隨機號碼產生器電路200包括一第一記憶體201，其可為一SRAM記憶體陣列，包含複數個記憶體單元，或者儲存元件。記憶體201適於連接之一電源202，該電源202可向該記憶體提供一可為VDD的電壓源。較佳的係記憶體201為非揮發性的並可操作以產生一第一信號206作為一輸出，該信號可為一未校正隨機號碼，其為該記憶體中該複數個記憶體單元之分別的初始狀態之一功能。

應理解一般而言SRAM不被認為係非揮發性記憶體，因為常規使用的SRAM中儲存的資料在該記憶體被切斷電源(即當該SRAM被斷電)時將丟失。然而，根據本發明描述於此之教旨，SRAM作為一非揮發性儲存媒體而被用於產生一安全隨機號碼，因為當每次該記憶體被供電時在該SRAM中該等記憶體單元之至少一部分將具有相同的(即可重複的)初始狀態。

記憶體201中的該等記憶體單元可被配置於例如一 $N \times M$ 之陣列中，其中 N 及 M 都為整數。本發明不限於記憶體201中該等記憶體單元的任何特定尺寸及/或配置。僅藉由顯

示之方式，記憶體201可包括一16字乘以32位元的陣列(16×32陣列)。此配置需要16個記憶體讀取週期，各個讀取週期產生一個32位元之資料字，以產生512位元之資料。隨機號碼產生器電路200可包含一控制器205，其可被耦合至記憶體201以控制對該記憶體中該等記憶體單元的存取。在一個實施例中，技術熟練者所熟知的係控制器205可包括列及/或行相關電路系統。或者，記憶體201中之該等記憶體單元可被配置於一個M個單元之單個列(例如一1×M陣列)中。舉例來說，在此情況下，記憶體201可包括M個並聯發生作用的單獨鎖存(未被明確顯示)。M個記憶體單元之整個列可被同時讀取於一單個記憶體讀取週期中，使用此配置的記憶體單元，所要求的該控制電路系統可被最小化或不需，在此情況下控制器205可被消除。然而，此配置要求一非常多的感測放大器以同時讀取該等記憶體單元之狀態，這可增加該IC之總面積及成本。

較佳的係資料字在該記憶體被供電(例如VDD被施加至該記憶體之後的一規定時間)之後及該記憶體之一初始狀態被建立之後從記憶體201讀取。較佳的係讀取記憶體201能從該記憶體將資料字傳送至該隨機號碼產生器電路200中之後的處理電路，其中未校正隨機號碼206係基於該等資料字。

隨機號碼產生電路200進一步包含一耦合至記憶體201的錯誤校正電路203。如前所述，在記憶體201中一記憶體單元子集具有在一給定資料字中的不明確初始狀態，其將以

其他方式產生一不會基於該記憶體之供電而一直重複的未校正隨機號碼206。較佳的係錯誤校正電路203可操作以校正由具有不確定初始狀態之記憶體單元產生的資料字使得所有從記憶體201讀取之資料位元將為確定的(可重複)。因此，一由錯誤校正電路203產生的可為一校正隨機號碼的第二信號207將係隨機的但可重複。較佳的係由該隨機號碼產生器電路200產生的該輸出安全碼為該校正隨機號碼207之一功能。

依據被錯誤校正電路203利用的錯誤校正方法，一可為一錯誤碼記憶體的第三記憶體204可視情況耦合至該錯誤校正電路。記憶體204較佳的係非揮發性的並可操作以儲存被該錯誤校正方法所使用之ECC位元。較佳的係這些ECC位元在當該安全碼(隨機號碼)被建立之時間中的某一點時被編程至記憶體204中。這可為在裝置工廠或用戶測試時或在此之後不久。這些ECC位元只需編程一次，然而若需要重設該安全碼，亦可在稍後將其重新編程。根據本發明之一實施例，記憶體204被初始供電記憶體201編程並在編程時儲存記憶體201中之該等記憶體單元的初始狀態。這些編程狀態被認為係記憶體201之該「校正」狀態。在之後的供電時，記憶體201中的該等記憶體單元之初始狀態將與儲存於記憶體204中的該「校正」狀態比較，且任何不與該等被儲存之狀態匹配的不明確位元將被錯誤校正電路203校正。

在本發明之多個實施例中，錯誤校正電路203可在產生

該校正隨機號碼207時利用例如一分組碼(例如一漢明碼)、一RS碼、一BCH碼等，雖然本發明不限於一特定的錯誤校正方法。當記憶體201被配置為一單個列的記憶體單元，較佳的係一RS碼或BCH碼被錯誤校正電路203使用，因為RS及BCH碼通常需要一相對較長的資料位元串以檢測及校正錯誤的資料位元。某些錯誤校正技術在可校正位元的數量及/或配置上具有限制。舉例來說，漢明碼雖然易於實施，但其只能為每個資料字校正一個位元錯誤。因此在一規定資料字中位元數量相對較小(例如少於16位元)的情況下較佳的係漢明碼。其他被錯誤校正電路203使用的錯誤校正技術可不需要儲存一記憶體碼，因此記憶體204可被省略。

現在參考圖3A，根據本發明之一實施例一種對顯示於圖2中之該錯誤碼記憶體204編程的示例性方法被顯示。方法300可被用於設置在記憶體201中具有不明確初始狀態(見圖2)之該等記憶體單元的「校正」狀態，該方法300之至少一部分可被執行於錯誤校正電路203中。以這種方式，較佳的係方法300被用以教正從記憶體201產生之該未校正隨機號碼206中的不會重複位元。使用於此之一術語「不會重複位元」旨在廣泛到涉及記憶體201中一規定記憶體單元之不具有一始終如一之初始狀態的一個輸出，使得基於電力對該記憶體的連續施加，該規定記憶體單元之初始狀態不必與該規定單元在電力對該單元的一或多個先前施加時的初始狀態相同。

為編程該錯誤碼記憶體204，記憶體201首先在步驟302中供電。在步驟303中，記憶體201被讀取以便基於未校正隨機號碼206產生一第一隨機號碼，該隨機號碼被轉發至錯誤校正電路203。此第一隨機號碼可包含不會重複之位元。在步驟304中，錯誤校正電路203產生一代表該第一隨機號碼的錯誤校正碼208。在步驟305中，該錯誤校正碼208被編程至錯誤碼記憶體204中。如前所述，該錯誤校正碼208可為一用於各個從記憶體201讀取之資料字的漢明碼。在對錯誤碼記憶體204編程後，每次記憶體201被供電時，該錯誤校正碼208被使用以檢測並校正任何錯誤位元以產生該校正隨機號碼207。因此，被錯誤校正電路203產生之校正隨機號碼207將係隨機但可重複的。

圖3B顯示根據本發明之一實施例一種再傳呼一校正隨機號碼(例如圖2中之207)之示例性方法320的步驟。較佳的係再傳呼被執行於錯誤碼記憶體204例如使用圖3A所顯示之方法300編程之後。方法320藉由步驟322中的記憶體201供電而開始。在供電時，該未校正資料字中所有位元的初始狀態被建立。在步驟323中，一第二隨機號碼基於從記憶體301讀取的該未校正隨機號碼206而被產生。因為不會重複之位元，該第二隨機號碼可與在結合圖3A而描述於上的該錯誤碼記憶體編程方法300期間產生的該第一隨機號碼不同。在步驟324中，該錯誤校正碼208從錯誤碼記憶體204中讀取。利用此錯誤校正碼208，在該第二隨機號碼中狀態與該第一隨機號碼中之相應狀態不匹配的任何不會重

複位元被校正於步驟325中，該等不會重複位元由該被儲存之錯誤校正碼指示。該校正隨機號碼207將從該第二隨機號碼產生。其將係與在該編程方法300期間產生的該第一隨機號碼相同的號碼。在步驟323中，如果該第二隨機號碼被測定為與在步驟300中產生的該第一隨機號碼相同，校正不需被執行。在此情況下，步驟324及325可被省略。

本發明之該等技術的至少一部分可被執行於一或多個積體電路中。在積體電路的形成中，典型的係晶粒以一種重複的型樣製造於一半導體晶圓之一表面上。各個晶粒可包含一種描述於此之裝置，亦可包含其他結構或電路。單獨的晶粒可從該晶圓上割下或切下，然後被封裝為積體電路。圖4為一部分截面圖，其顯示一包括至少一個根據本發明之一實施例之安全隨機號碼產生器電路的示例性封裝IC400。該封裝IC包括一引線架402、一附接至該引線架的晶粒404及一塑膠封裝模408，該晶粒包含一根據本發明之一實施例的安全隨機號碼產生器。技術熟練者知道如何切割晶圓及封裝晶粒以製造積體電路。如此製造之積體電路被認為係本發明之一部分。

一種根據本發明之積體電路可被使用於利用安全碼的任何應用及/或電子系統中。可實施本發明的合適系統可包含，但不限於，個人電腦、通信網路、電子商務系統、可攜式通信裝置(例如行動電話)、固態媒體儲存裝置等。包含如此之積體電路的系統被認為係本發明之一部分。在給

出提供於此之本發明的教旨之前提下，一般技術者能考慮本發明之技術的其他實施方式及應用。

雖然本發明之說明性實施例參考該等圖式而被描述於此，應理解本發明不限於任何確切的實施例，技術熟練者可在這些實施例中做出多種其他變化及修改而不脫離該等請求項之範圍。

【圖式簡單說明】

圖1為一可結合於本發明之一實施例而使用的示例性靜態隨機存取記憶體(SRAM)陣列之一概要圖。

圖2為一根據本發明之一實施例的示例性隨機號碼產生器電路之一方塊圖。

圖3A顯示根據本發明之一實施例一種對顯示於圖2中之該錯誤碼記憶體編程之示例性方法的步驟。

圖3B顯示根據本發明之一實施例一種再傳呼一校正隨機號碼之示例性方法的步驟。

圖4為一部分截面圖，其顯示一包括至少一個根據本發明之一實施例之安全隨機號碼產生器電路的示例性封裝IC。

【主要元件符號說明】

18	SRAM陣列
20	SRAM單元
30	電晶體裝置
32	電晶體裝置
34	節點

36	節 點
40	電 晶 體 裝 置
42	電 晶 體 裝 置
46	電 晶 體 裝 置
48	電 晶 體 裝 置
200	隨 機 號 碼 產 生 器 電 路
201	記 憶 體
202	電 源
203	錯 誤 校 正 電 路
204	錯 誤 碼 記 憶 體
205	控 制 器
206	未 校 正 隨 機 號 碼
207	校 正 隨 機 號 碼
208	錯 誤 校 正 碼
300	方 法
302	步 驟
303	步 驟
304	步 驟
305	步 驟
320	方 法
322	步 驟
323	步 驟
324	步 驟
325	步 驟

400	積體電路
402	引線架
404	晶粒
408	塑膠封裝模

十、申請專利範圍：

1. 一種隨機號碼產生器電路，其包括：

一具有複數個儲存元件的第一記憶體，當被一施加至該第一記憶體的電壓供應源供電時，該複數個儲存元件之每一者具有一與其相應的初始狀態，該第一記憶體可操作以產生一第一信號，該第一信號包含複數個指示該複數個儲存元件之各別初始狀態的位元；及

一耦合至該第一記憶體的錯誤校正電路，該錯誤校正電路可操作以接收該第一信號及校正該第一信號中至少一個不會基於電力對該第一記憶體之連續施加而重複的位元以便藉此產生一第二信號，該第二信號係一個可基於電力對該第一記憶體之連續施加而重複的隨機號碼；

其中該複數個儲存元件之該等各別初始狀態包含在該複數個儲存元件被供電之後及在該複數個儲存元件被寫入之前該複數個儲存元件所在之各別狀態。

2. 如請求項1之隨機號碼產生器電路，其中該第一記憶體包括非揮發性記憶體。

3. 如請求項1之隨機號碼產生器電路，其中該第一記憶體包括靜態隨機存取記憶體。

4. 如請求項1之隨機號碼產生器電路，其進一步包括一耦合至該錯誤校正電路的第二記憶體，該第二記憶體可操作以儲存該錯誤校正電路在該第二信號的產生中所使用的若干錯誤校正碼位元。

5. 如請求項4之隨機號碼產生器電路，其中該等第一及第

二記憶體中的至少一者包括一非揮發性記憶體。

6. 如請求項1之隨機號碼產生器電路，其中該複數個儲存元件之至少一個子集中的每一者係包括一互補金屬氧化物半導體電路元件。
7. 如請求項1之隨機號碼產生器電路，其中該複數個儲存元件之至少一個子集中的每一者係包括一鎖存元件。
8. 如請求項1之隨機號碼產生器電路，其中該複數個儲存元件包括若干靜態隨機存取記憶體元件，且其中該第一記憶體直到該第一記憶體被該電源供電之後且該第一記憶體產生該第一信號才被寫入。
9. 如請求項1之隨機號碼產生器電路，其進一步包括一耦合至該第一記憶體的控制器，該控制器可操作以控制對該複數個儲存元件的存取。
10. 如請求項1之隨機號碼產生器電路，其中該複數個儲存元件之一給定者的初始狀態係隨與形成該給定儲存元件之至少一電晶體相關聯之一或多個特徵中之差異的改變而予以測定。
11. 如請求項10之隨機號碼產生器電路，其中該一或多個特徵包括以下至少一者：該至少一電晶體源極及汲極區域內的摻雜位準、該電晶體通道區域內的摻雜位準、電晶體閘極氧化物電容、電晶體閘極氧化物中的捕獲電荷、該電晶體通道區域中的捕獲電荷、以及在各電晶體區域之間的幾何偏移、電晶體通道長度及電晶體通道寬度。
12. 如請求項1之隨機號碼產生器電路，其中該複數個儲存

元件之一給定者之初始狀態係隨在一或多個時變元件中之差異的改變而予以測定，該差異係包括溫度、供應電壓位準、供應電壓轉換率及電雜訊中之至少一者。

13. 如請求項1之隨機號碼產生器電路，其中該錯誤校正電路在產生該第二信號時係利用一分組碼、一裏德-所羅門碼及一博斯-喬赫裏-霍克文黑姆碼中的至少一者。

14. 一種包括至少一個如請求項1之隨機號碼產生器電路的積體電路。

15. 一種產生一安全隨機號碼的方法，該方法包括如下步驟：

對一包括複數個儲存元件的第一記憶體供電，當被供電時該複數個儲存元件之每一者具有一與其相應的初始狀態；

產生一第一信號，該第一信號包括複數個指示該複數個儲存元件之分別初始狀態的位元；及

校正該第一信號中基於電力對該第一記憶體的連續施加不會重複的至少一個位元以便藉此產生一第二信號，該第二信號係一個可基於電力對該第一記憶體之連續施加而重複的隨機號碼，該安全隨機號碼係對該第二信號的指示；

其中該複數個儲存元件之該等各別初始狀態包含在該複數個儲存元件被供電之後及在該複數個儲存元件被寫入之前該複數個儲存元件所在之各別狀態。

16. 如請求項15之方法，其進一步包括在一第二記憶體中儲

存若干錯誤校正碼位元的步驟，該等錯誤校正碼位元係在產生該第二信號時被使用。

17. 如請求項15之方法，其進一步包括：

第二次對該記憶體供電，其中該記憶體產生一第二隨機號碼；

在一第二記憶體中讀取該錯誤校正碼；及

使用該錯誤校正碼校正該第二隨機號碼，其中該經校正之第二隨機號碼係該第一隨機號碼。

18. 如請求項15之方法，其中該複數個儲存元件之一給定者的初始狀態係隨與形成該給定儲存元件之至少一電晶體相關聯之一或多個特徵中之差異的改變而予以測定。

19. 如請求項15之方法，其中該複數個儲存元件之一給定者之初始狀態係隨在一或多個時變元件中之差異的改變而予以測定，該差異係包括溫度、供應電壓位準、供應電壓轉換率及電雜訊中之至少一者。

20. 一種電子系統，其包括：

至少一個積體電路，該積體電路包含至少一個隨機號碼產生器電路，該至少一個隨機號碼產生器電路包括：

一具有複數個儲存元件的第一記憶體，當被一施加至該第一記憶體的電壓供應源供電時，該複數個儲存元件之每一者具有一與其相應的初始狀態，該第一記憶體可操作以產生一第一信號，該第一信號包含複數個指示該複數個儲存元件之各別初始狀態的位元；及

一耦合至該第一記憶體的錯誤校正電路，該錯誤校正

電路可操作以接收該第一信號及校正該第一信號中至少一個不會基於電力對該第一記憶體之連續施加而重複的位元以便藉此產生一第二信號，該第二信號係一個可基於電力對該第一記憶體之連續施加而重複的隨機號碼；

其中該複數個儲存元件之該等各別初始狀態包含在該複數個儲存元件被供電之後及在該複數個儲存元件被寫入之前該複數個儲存元件所在之各別狀態。

十一、圖式：

18

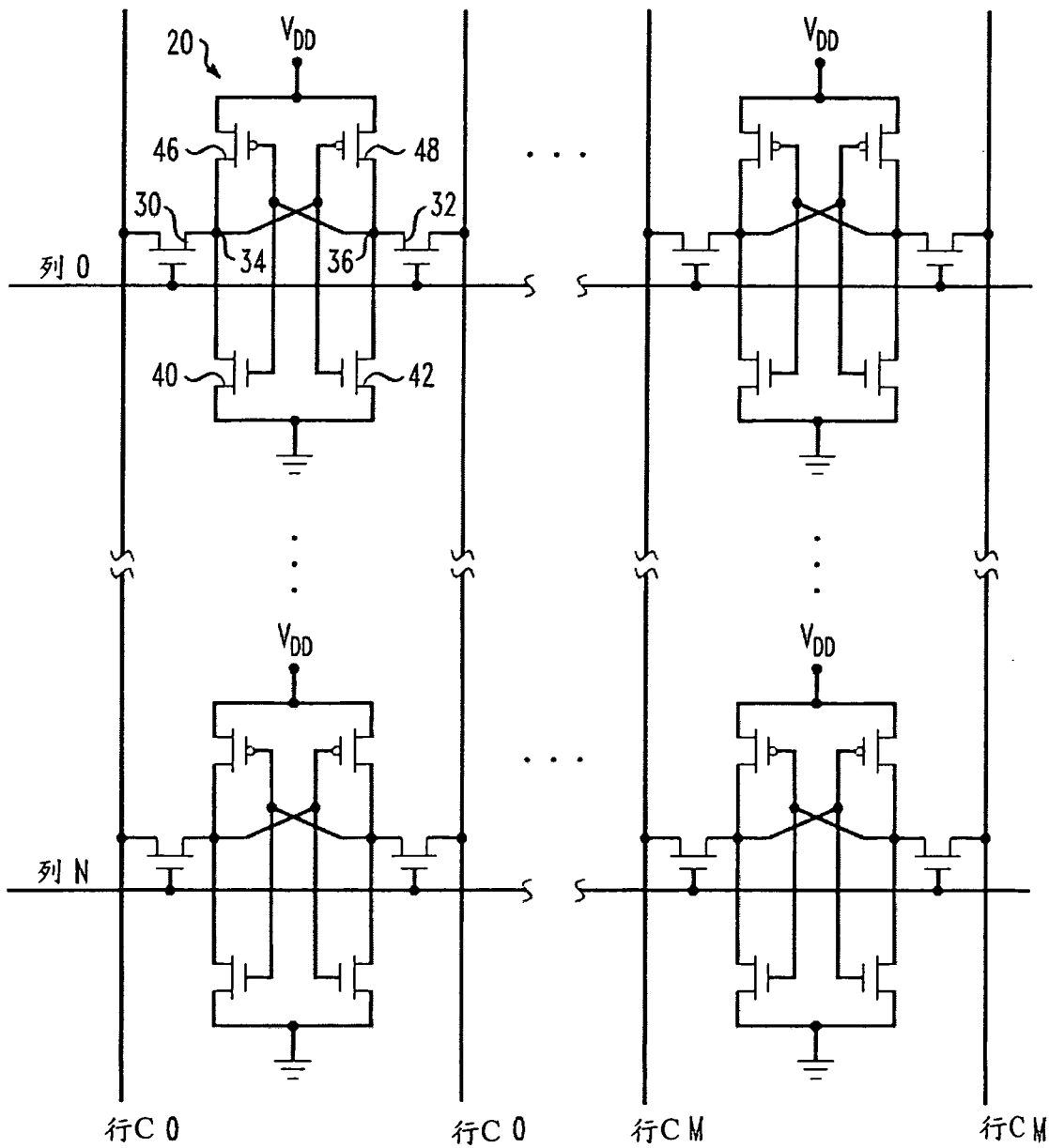


圖 1

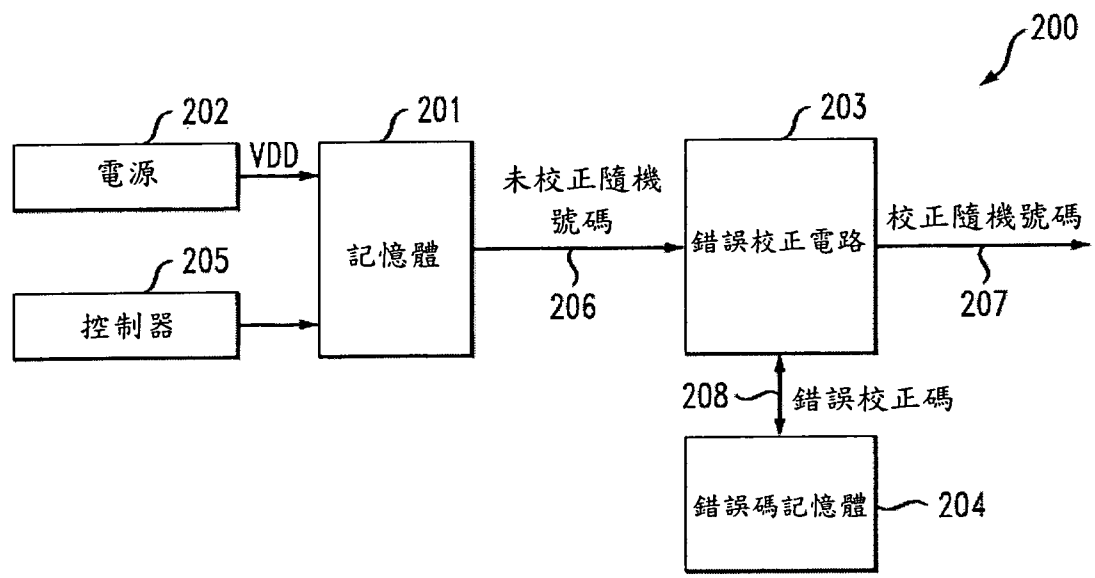


圖 2

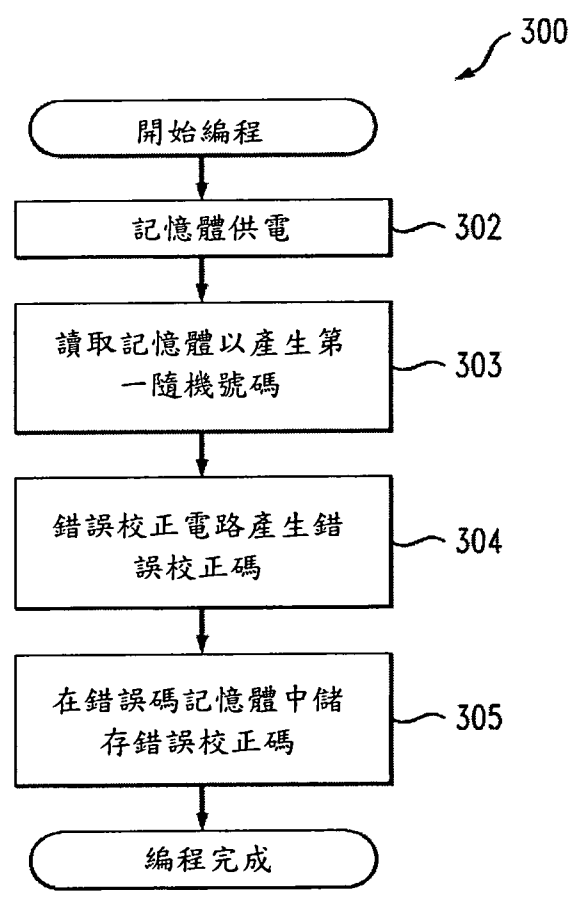


圖 3a

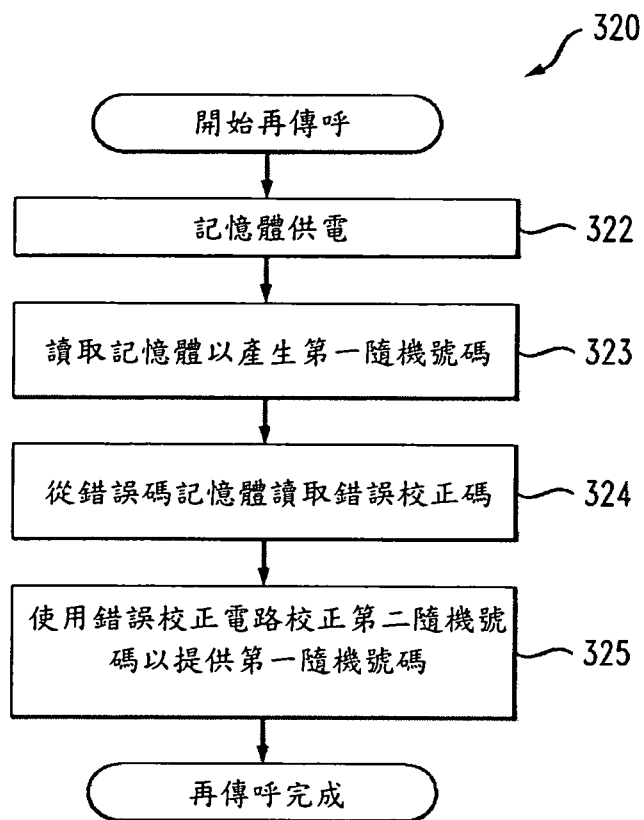


圖 3b

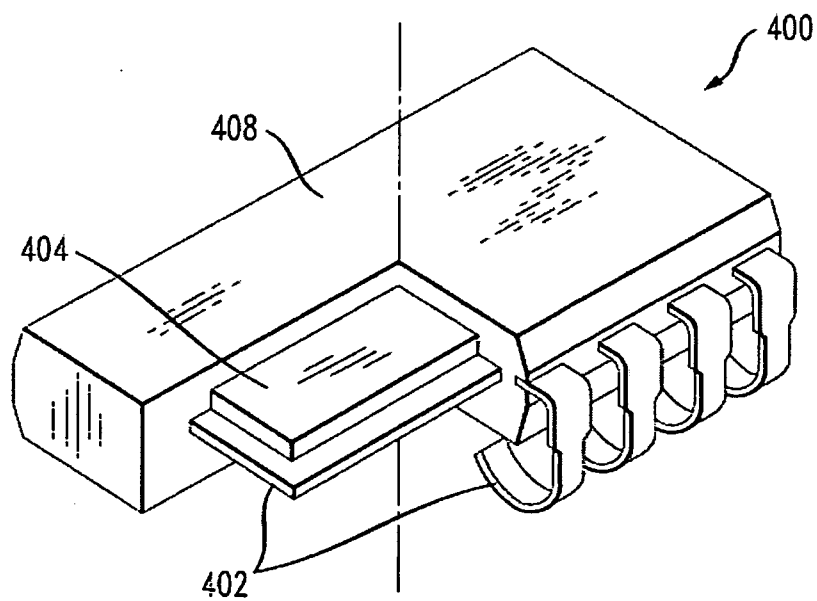


圖 4