快速、安全、低成本的加解密解決方案

仿生物智慧型加解密單晶片
Bionic Intelligent Cipher Chip

陳慶瀚

義守大學MIAT實驗室

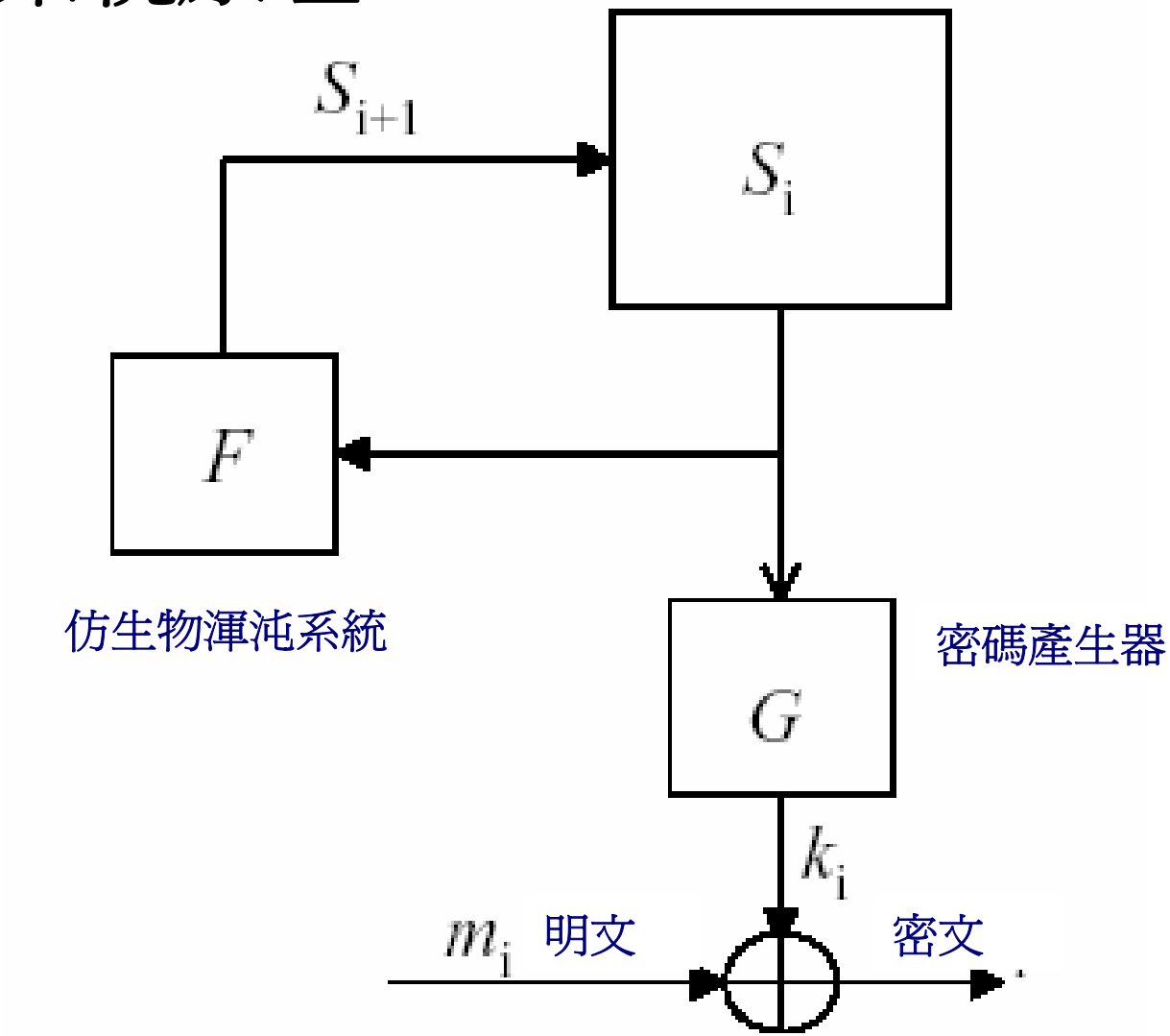
簡述:

- 本晶片採用無法被破解的韋南(Vernam)加密概念，藉由一個Chaos系統， 來產生與明文資料相同長度的絕對亂數的密碼鑰匙，每一次使用的密碼鑰匙都由系統演化生成。由於Chaos系統對於初始條 件的高度敏感，演化初值的微小變異會導致完全不同的演化方向，進而確保了密碼的不可預測性。

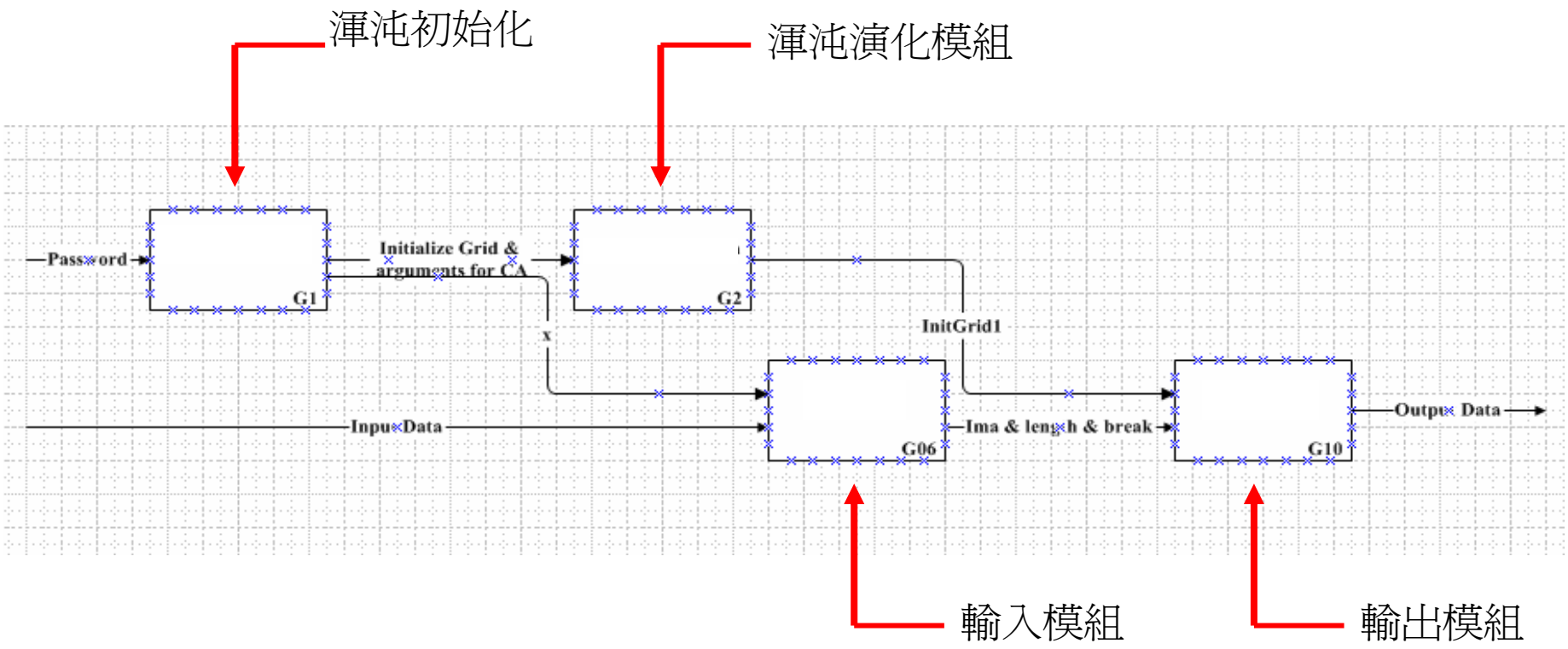
隱密性及安全性:

- 在雙方或多方加解密的情況下，爲達到密鑰同步的要求，「仿生物智慧型加解密系統晶片」利用演化的機制，在相同的起始條件及相同的演化環境下，方能得到相同的密鑰。也就是說密鑰是存在於系統的本身，不會因密鑰的傳輸而外曝。另外，密鑰同時可藉由「仿生物智慧型加解密系統晶片」本身及使用者外部的設定來加以變更，使得各系統間擁有不同的演化特性。讓同爲使用本產品的不同系統之間，仍能保有各自的隱密性及安全性。讓整體在安全防護上更牢不可破。

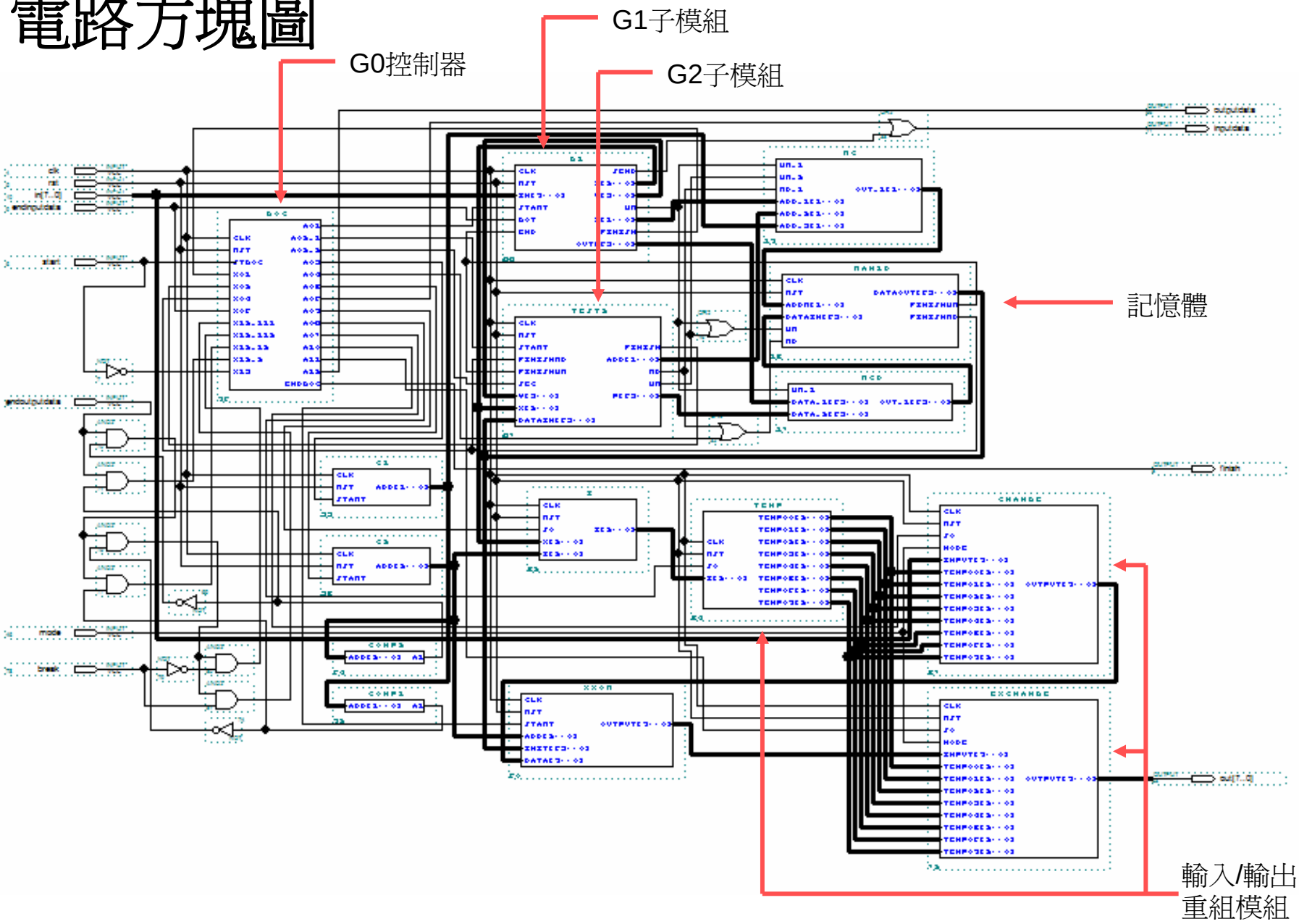
系統原理



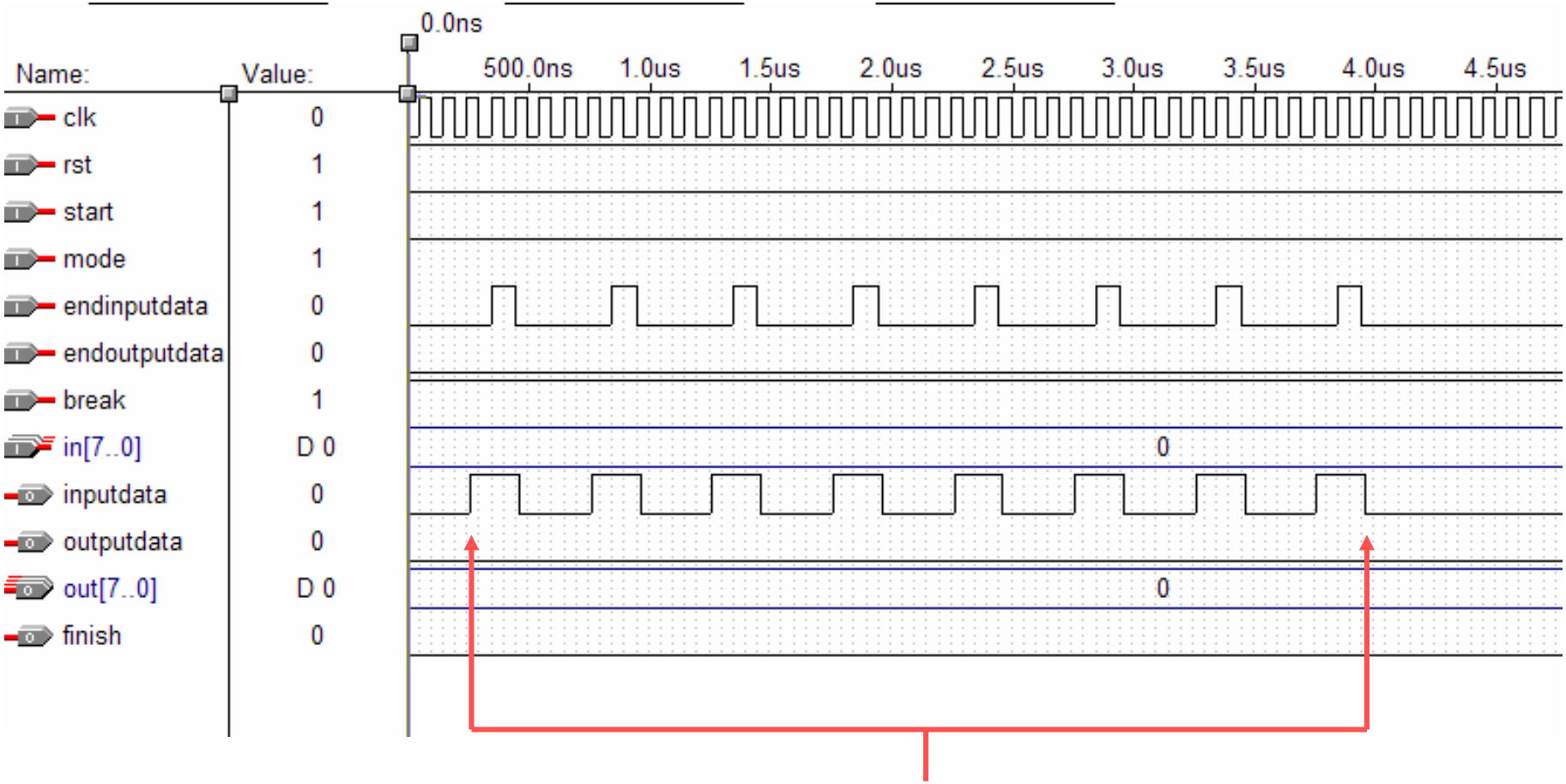
系統架構


渾沌初始化
渾沌演化模組
Password
G1
Initialize Grid &
arguments for CA
G2
x
InitGrid1
Input Data
G06
Ima & length & break
G10
Output Data
輸入模組
輸出模組

電路方塊圖

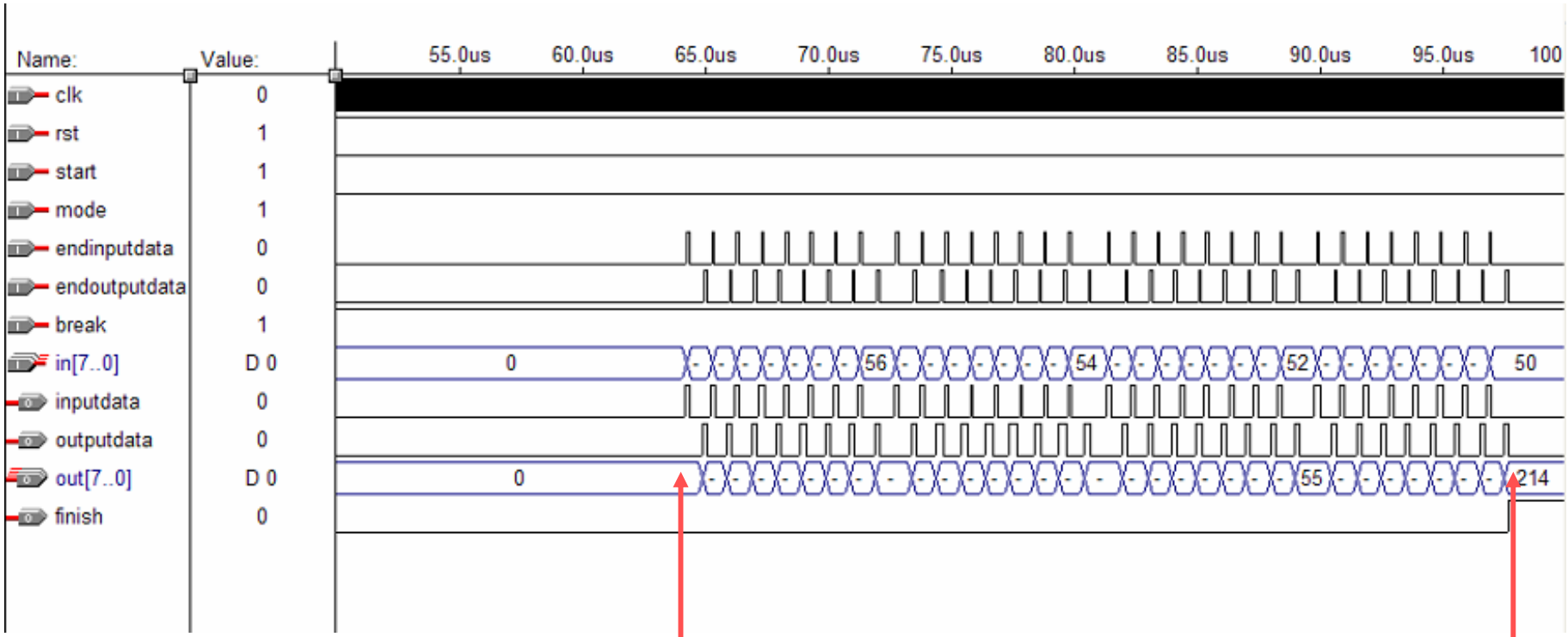


渾沌初始化功能時序圖



8次共16位密碼

資料I/O功能時序圖



一輪爲 **256 bits** 資料

晶片規格:

- I/O:
  8 bits data & **6 bits** control **Input**
  8 bits data & **3 bits** control **Output**
- Gate Counts:
  ~ 1,7092
- Speed:
  maximum **1.8MB/s** at **25.38MHZ**

晶片接腳:

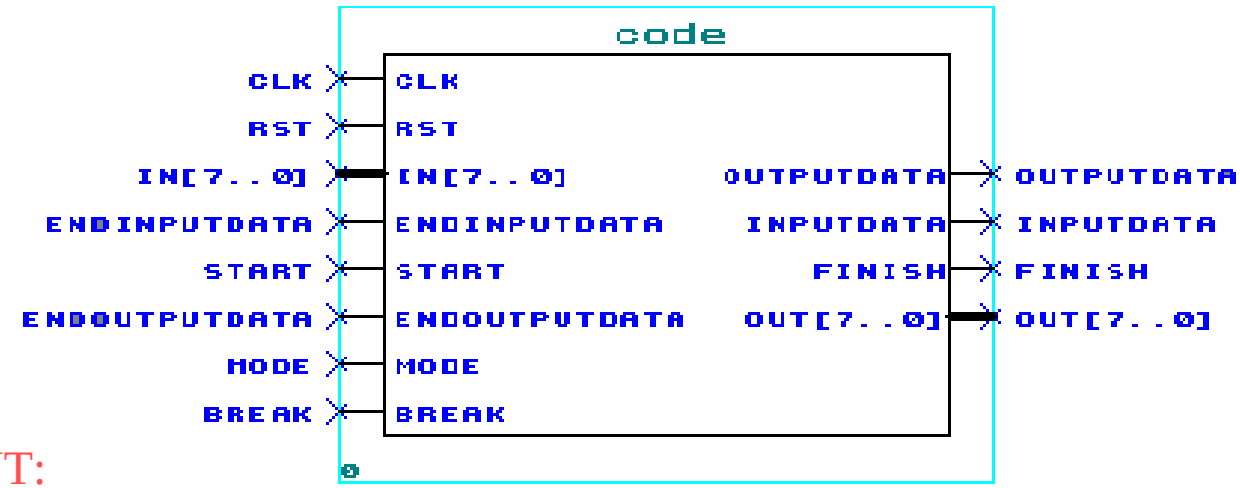
OUTPUT:

OUTPUTDATA: 輸出資料備妥

INPUTDATA : 要求資料輸入

OUT[7..0]: 資料 8 bits

FINISH: 結束訊號



INPUT:

CLK: 時脈

RST: 重置

IN[7..0]:資料 8 bits

MODE: 加/解密模式

ENDINPUTDATA: 輸入資料備妥

ENDOUTPUTDATA:輸出資料處理結束

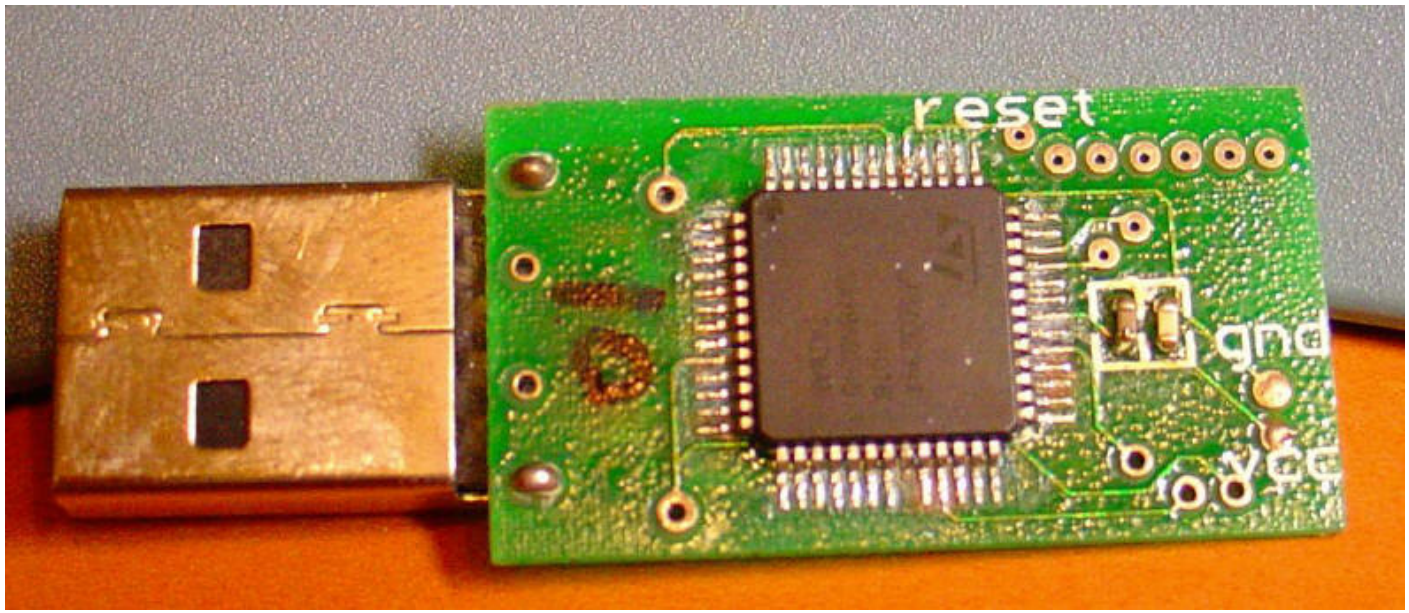
START: 起始訊號

BREAK: 中斷訊號

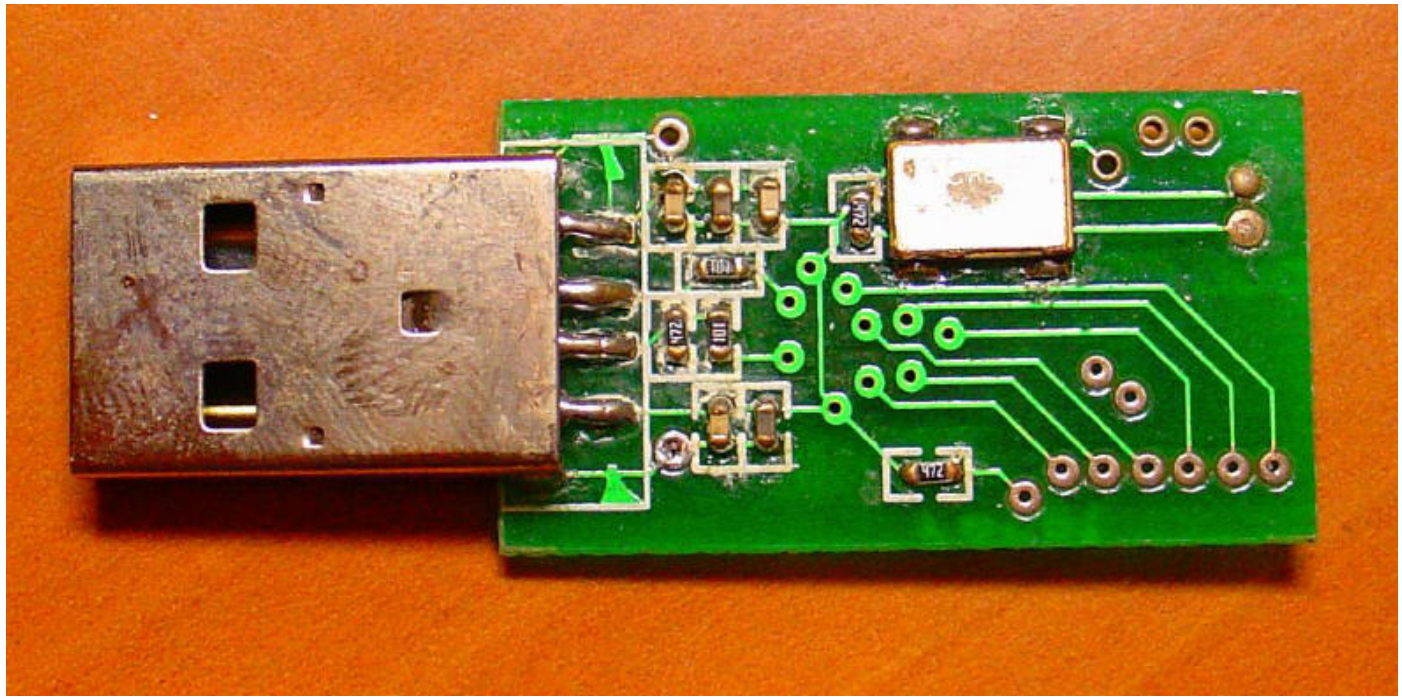
晶片特色:

- 使用**256bits**的渾沌初始密鑰，以此演化出與明文相同長度的密鑰，具有最高的安全性。
- 採用**on-the-fly**生成串流式密鑰，結構精簡，無須儲存密鑰空間，且倍增其安全性。
- 加解密過程以**one-shot**模式進行，沒有複雜的疊代或算術運算，爲當今最快速的加解密方法。
- 基於**非線性**和**複雜動力學**的加密程序，確保無法由密文逆推本文的不可破譯特性。
- 晶片**成本低廉**，**體積小**、易於整合。

產品照片(正面)：



產品照片(背面)：



應用範圍：

- 在無線傳輸環境，資料曝露在public channel中，極易被攔截、竊取或竄改，「仿生物智慧型加解密系統晶片」提供一個絕對安全的保密傳輸解決方案。
- 對於需要即時加解密的大量影音資料通訊系統，「仿生物智慧型加解密系統晶片」，提供了最高速的加解密解決方案。
- 各種可攜式資料儲存裝置，「仿生物智慧型加解密系統晶片」可在幾乎不減低效能的情況下，提供最低成本、最高安全性的資料保護解決方案。
- 在公文秘件或個人隱私的公共資料庫、資訊安全系統或生物辨識系統，「仿生物智慧型加解密系統晶片」均能提供高私密性及高效率的完全安全防護解決方案。

應用產品開發方向：

- 可攜式USB-解密；
- MP3/MPEG-4即時解密撥放器；
- 加解密隨身碟；
- 高安全度的WLAN ；
- 隨選視訊(Set-Up Box)加解密。