

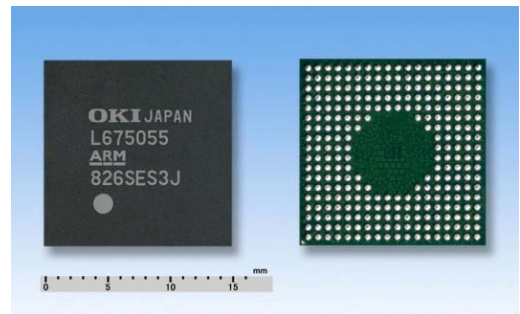
2009 年 1 月 20 日

開發出了適用於刷卡機的高安全性能的 LSI、ML675055 搭載了支援 PCI-PED2.0 的加密技術

OkI Semiconductor 此次新開發了「ML675055」，自本日起開始發售。OKI 將特有的 IP 群(符合刷卡機安全度評價標準 PCI-PED2.0(*1) 的高安全性能的 IP 群)與適當的外圍控制功能集成在了單片晶片「ML675055」中。

OkI Semiconductor 特有的加密 IP 群由以下構成：耐受各種攻擊(*2)、能安全的進行加密・解密的密碼引擎，對攻擊進行監控的各種傳感器、以及在惡性程序下保護密鑰等重要數據的存儲器保護功能。ML675055：在 ARM7 為基礎的 32bit

高性能 CPU 內核中搭載了 8Kbyte 的高速緩沖存儲器 (cache memory)，在頻率為 80MHz 的系統 LSI 中集成了 OKI 特有的加密 IP 群，並將結算終端所必需的各種相關功能都集中在單片晶片上。本 LSI 通過了世界上權威的 PCI-PED 安全性能評估實驗室—德國「T-Systems」的安全性評估(assessment)，適用於 PCI-PED2.0 的機器認證所必需的 PED(*3)、信用卡認證終端(CAT)等。



【開發背景】

隨著全球對個人信息保護的關心度的提高，以及信用卡犯罪的不斷智能化，複雜化，要求我們不應僅限於以前的 IC 卡交易的保護，還應提高 PED 等終端設備整體的安全性。敝公司在符合新安全規格的終端設計方面，為了盡可能的減輕客戶的負擔，以將加密相關的功能最大限度的集中在 LSI 內部為目標，致力於加密技術的研發。因此，我們開發了高防解密(*4)的加密 IP 群、並開始發售搭載了此 IP 群的 LSI、ML675055。OKI 今後會繼續推出搭載這些 IP 群的 LSI 商品。

【本 LSI 產品的特點】

- 內置新開發的防解密的加密 IP 群
搭載了耐電量分析(*5)的 RSA(*6)、DES/T-DES(*7)、AES(*8)、SHA1/SHA256(*9)的各種密碼引擎、能夠高速且安全的運行。特別是 RSA，能夠用最大 2112bit 的密鑰鍵進行加密、解密運算。另外，搭載了電壓，溫度，頻率等各種傳感器、通過對這些進行監控，進而實現防解密。控制獨自開發的存儲器保護功能，檢測出由於不正當訪問引起的攻擊。
- 32bitCPU 內核、ARM7TDMI 為基礎、80MHz 的高速動作
作為 CPU 內核，採用業界標準的 ARM7TDMI，搭載 8Kbyte 的高速緩沖存儲器 (cache memory)，能夠進行 80MHz 的高速動作。

- 有安全的外部存儲器接口能夠進行拓展
提供具備獨立密碼結構的外部存儲器接口。能夠滿足客戶大容量的應用程序及數據的需求。
- 對 PCI-PED2.0 實施第三方評估(assessment)
關於配置各種加密功能，由世界權威的 PCI-PED 認證實驗室：德國「T-Systems」進行安全評估。
由於有公正的評價數據，能夠減少客戶採用該產品時的評估作業，令客戶放心。

依據評價報告，提供終端設計指南

根據評價得出的評價結果，將加密實裝的 guideline 作為應用備忘錄提供給客戶。

- 能够以单片晶片實現終端功能的豐富的外圍接口
搭載了以 Full-Speed(12Mbps)動作，USB2.0 標準的 host/device，由於是不同的接口所以能夠同時使用。將用於 4 張 IC 卡或 SIM 卡的控制器、大容量 NAND flash 控制器、用於顯示認證信息的 LCD 控制器、UART 及 I2C、SPI 等的系列控制器集成起來，在單晶片實現了豐富的外圍功能。

【銷售計劃】

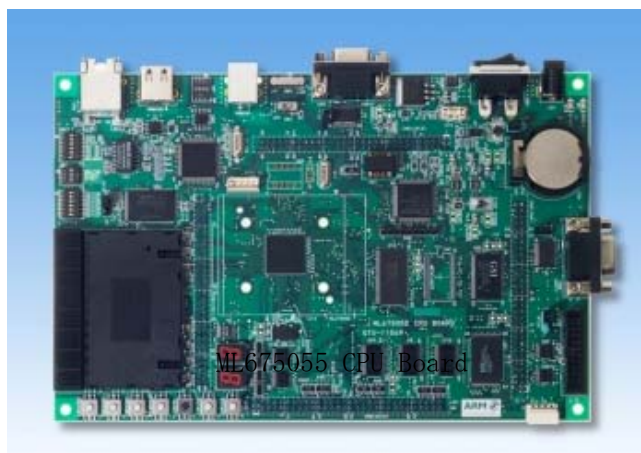
- 產品名：ML675055
- 樣品：受理訂貨
- 量產出貨時間：2009 年 1 月
- 軟體開發工具(SDK)：受理訂貨

【ML675055 的主要規格】

- 加密 IP 群 : 支持各種密碼引擎
RSA(不使用CRT^{(*)10})的最大 2112bit的加密，解密鑰)、
DES/T-DES、AES、SHA1/256
密鑰的耐電量分析(DPA/SPA)性
通過內置傳感器監控攻擊
搭載自主開發的存儲器保護結構
- IC 卡控制器 : 參照 ISO7816、搭載 4ch
符合 EMV(4.0) 標準
- serial interface : USB2.0 標準的 host interface(Full-Speed)
USB2.0 標準的 device interface(Full-Speed)
搭載 UART 4ch、I2C 2ch、SPI 2ch
- 應對大容量存儲 : 內置 NAND flash 控制器
- 顯示控制 : 內置 QVGA 黑白液晶控制器(VRAM 內置)
- CPU 內核、頻率 : ARM7TDMI(+8Kbyte Cache)、80MHz
- 內置 RAM : 最大 32Kbyte 搭載
- 外部存儲器接口 : FLASH、ROM、SDRAM、可控制各種 I/O
(通過密碼對存儲器 device 進行保護)
- 通用 I/O 端子 : 最多可使用 148bit
- 其他外圍功能 : 搭載各種計時器、A/D 轉換器
- 封裝 : 272pin LFBGA (15mm□)

【ML675055 軟件開發工具包 (SDK)】

ML675055 軟件開發工具包 (SDK) 即：用於支持採用了 ML675055 的 IC 卡終端及結算終端等加密系統開發的軟件開發工具包。本產品由以下構成：ML675055 的 CPU 板、與 CPU 板組裝使用的 baseboard、能夠確認 ML675055 各種功能的示例軟件，用於開發的各種實用工具。詳細資敬請詢問。



【術語說明】

- (*1) PCI-PED2.0 : 針對信用卡結算時用來輸入 PIN(識別密碼)的機器，對其物理上的，邏輯上的安防條件進行規定的國際標準。
目前，版本 2 是最新標準。
- (*2) 各種攻擊 : 是指物理攻擊 (DFA、惡性程序的運行、異常環境下誤動作的發生等)、旁道 (Side channel) 攻擊 (電力分析等)。
DFA(Differential Fault Analysis)是指、在進行密碼處理時，通過給 LSI 印加異常狀態 (電壓與溫度等)、向 clock 端子印加脈沖 (glitch) 等，令其運作發生故障 (計算錯誤)，通過判斷正常運作時與故障運作時的輸出的不同來推算出密鑰的攻擊。
- (*3) PED : PIN Entry Device 的縮寫。識別密碼輸入裝置
- (*4) 防解密 : 物理上的或是邏輯上的，對於被讀取 LSI 內部信息的耐受性。
- (*5) 電量分析 : 著眼於 LSI 在進行處理時的晶片的消耗電量與處理信息的邏輯值有相關關係這一點，通過觀察消耗電量來推算出密鑰的方法。
常見的方法為：直接解析密碼處理過程中消耗電流波形的變化，來推算出密鑰的方法 (SPA: Simple Power Analysis)、以及對多數的消耗電流波形、進行統計處理，來推算出密鑰的方法 (DPA: Differential Power Analysis)。
- (*6) RSA : 非對稱密碼算法之一。公鑰密碼中使用的算法。
RSA 是定義該算法法則的三個人的名字 (Rivest, Shamir, Adleman) 的首個字母。
- (*7) DES/T-DES : 對稱密碼算法之一。DES: Data Encryption Standard、
T-DES: Triple DES。
- (*8) AES : 對稱密碼算法之一。AES: Advanced Encryption Standard。
- (*9) SHA1/SHA256 : 對稱密碼算法之一。SHA: Secure Hash Algorithm 是一群相關聯的 hash 函數。
根據生成的 hash 值的 bit 數的不同，有不同的種類。
SHA1 生成 160bit 的 hash 值、SHA256 生成 256bit 的 hash 值。
- (*10) CRT : Chinese Remainder Theorem (中國剩餘定理)
起源於中國的算術書「孫子算經」、是關於整數的剩餘的定理。
利用這個定理、可以拓展 RSA 密碼演算的密鑰，但在拓展的過程中、容易受到對密鑰的攻擊。

本文所提及的公司名稱、商品名稱均為各公司的商標或註冊商標。