**摘要**

論文名稱：用於預測心血管疾病的超低功耗的安全物聯網平台

頁數：三十九頁

校所別：國立臺北科技大學　電子工程系　研究所

畢業時間：一百零八學年度　第二學期

學位：碩士

研究生：林清河

指導教授：賴柏洲　教授

關鍵詞：物聯網1、能源效率2、安全/隱私3、 心電圖4、硬體安全5。

　　物聯網1（Internet of Things, IoT）承諾通過對患者的遠程，連續和非侵入性監控來徹底改變醫療保健行業。然而，IoT支持的醫療設備面臨兩個主要挑戰：能源效率2和安全/隱私3問題。研究人員已經獨立嘗試開發解決方案，例如低功率心電圖4 (Electrocardiography, ECG)處理器和安全協議，以便在個人基礎上解決這些挑戰。但是，必須研究以協同方式集成的整體解決方案，從而提供整體安全且節能的產品。在本文中，我們開發了一個超低功耗和安全的IoT傳感/預處理平台，用於使用心電信號預測室性心律失常。我們提出的解決方案能夠提前3小時預測關鍵心血管事件的發生率，準確率為86％。此外，所提出的架構是使用65納米低功率增強技術的專用集成電路設計流程設計的;它消耗的功率比最先進的方法低62.2％，而佔用面積減少16.0％。所提出的處理器利用ECG信號來提取芯片特定的ECG密鑰，該密鑰能夠保護通信信道。通過將ECG密鑰與現有的信任設計解決方案相集成，所提出的平台還在硬體級別提供保護，從而阻止硬體安全5威脅，例如逆向工程和偽造。通過有效共享芯片上資源，多層安全基礎設施的開銷保持在9.5％的面積和0.7％的功率，而不影響設計的速度

**ABSTRACT**

Thesis Title：Ultra-Low Power, Secure IoT Platform for Predicting Cardiovascular Diseases

Page：39

University：National Taipei University of Technology

Graduate School：Master Program, Department of Electronic Engineering

Date：May 8, 2019

Degree：Master

Graduate Student：Ching-Ho Lin

Advisor：Po-Chou Lai, *Prof*.

Keywords：Internet of Things1, energy-efficiency2, security/privacy3, ECG 4, hardware security5.

　　Internet of Things1 (IoT) promises to revolutionize the health-care sector through remote, continuous, and non-invasive monitoring of patients. However, there are two main challenges faced by the IoT-enabled medical devices: energy-efficiency2 and security/privacy3 concerns. Researchers have independently attempted to develop solutions, such as low-power ECG4-processors and security protocols, that address these challenges on an individual basis. However, it is imperative to investigate holistic solutions that integrate in a synergistic manner, delivering an overall secure and energy-efficient product. In this paper, we develop an ultra-low power and secure IoT sensing/pre-processing platform for prediction of ventricular arrhythmia using ECG signals. Our proposed solution is able to predict the on-set of the critical cardiovascular events upto 3 h in advance with 86% accuracy. Moreover, the proposed architecture is designed using an Application Specific Integrated Circuits design flow in 65-nm Low Power Enhanced technology; the power it consumes is 62.2% less than that of the state-of-the-art approaches, while occupying 16.0% smaller area. The proposed processor makes use of ECG signals to extract a chip-specific ECG key that enables protection of communication channel. By integrating the ECG key with an existing design-for-trust solution, the proposed platform offers protection also at the hardware level, thwarting hardware security5 threats, such as reverse engineering and counterfeiting. Through efficient sharing of on-chip resources, the overhead of the multi-layered security infrastructure is kept at 9.5% for area and 0.7% for power with no impact on the speed of the design.

**誌謝**

　　轉瞬間已經即將邁入二年級，碩士求學光陰轉瞬將過。在這段學習的時光中所學的不僅只是專業知識，在許多課程中所學到的是更多的思考與想法的訓練。研究成果非我一己之力所能達成，若非師長的引導，在茫茫的知識海洋中難以找到方向。

　　首先獻上由衷的感謝論文寫作指導　賴柏洲教授，在論文寫作課程方面給予嚴格的指導。也因為嚴格詳細的指導寫作方式，對於未來如何撰寫更加了解不會手足無措。這堂課並不只是用在論文書寫，也可用在書信往返及公司文件上。若格式撰寫錯誤百出，會讓閱讀文件的人貽笑大方且失了禮儀。感謝老師的諄諄教誨與對學生的關心。

　　感謝我的專題指導　李仁貴教授，每次的專題討論開會時對於專題報告的內容給予要點提醒。提醒了我如何抓住論文的重點，公式、方法背後的意義是什麼？是否是實際應用上能有所貢獻的還是只是紙上談兵？教授的指引往往都帶出重點，依循著指引更能精確地抓到方向。

　　感謝我的博士班學長吳昭畿，在專題方面給予的指導與協助，詳細一步步的講解相關的知識。當我遇到困難難以向前邁進時給予可能的建議，不斷的嘗試努力下有所突破。最後感謝我的家人及主管、同事支持與包容著我讓我在工作繁忙之餘能仍有機會到學校進修。如果沒有您們的支持一路走來將篳路藍縷。感謝您們的幫助使我終將完成碩士學業。感謝在研究專題過程中所有給予我協助的人，無法一一答謝，僅透過此論文表達最誠摯的感激之意。

林清河　謹致

臺北科技大學電子工程學系研究所

中華民國一百零八年九月

**目錄**

摘要 ……………………………………………………………………….. i

英文摘要 iii

誌謝 v

目錄 vi

圖目錄 viii

表目錄 ix

第一章 緒論 1

1.1物聯網和醫療保健 1

1.2可穿戴/植入設備的安全挑戰 1

1.3威脅模型 3

1.4目標：整體一體化 4

1.5建議的VA處理器 5

第二章 背景和相關工作 8

2.1以前關於ECG處理器的工作 8

2.2以前的硬體安全工作：邏輯鎖定 8

2.3關於ECG密鑰生成的先前工作 11

第三章 VA處理器架構 12

3.1心電圖預處理….… 13

3.2特徵提取階段 14

3.3分類階段….… 14

第四章 安全VA處理器 15

4.1安全目標 15

4.2識別要保護的處理器區塊 16

4.3安全VA處理器架構 17

4.4第1層：預測率操縱 18

4.5第2層：SAT攻擊彈性 21

4.6第3層：拒絕服務（Denial of Service, DSLL） 21

4.7第4層：ECG密鑰生成 22

4.8芯片專用密鑰生成 23

第五章 實驗與結果 24

5.1實驗框架 24

5.2表現結果 24

5.3 ASIC設計 25

5.4安全技術：鎖定對預測率的影響 27

5.5安全技術：執行時間 28

5.6安全技術：面積，功率，延遲開銷 29

第六章 討論和未來的工作 32

第七章 結論 33

第七章 研讀心得 34

參考文獻 35

**圖目錄**

圖1 IC設計流程中不同階段的新安全威脅 3

圖2 可佩戴的VA SoC處理和分析ECG資料 5

圖3 IC設計流程的邏輯鎖定 9

圖4 使用XOR / XNOR門進行邏輯鎖定 9

圖5 帶註釋ECG波形 11

圖6 心室心律失常預測系統示意圖 12

圖7 預處理階段的流程圖 13

圖8 提出的安全性心室心律失常預測處理器的結構 18

圖9 抽象表示RTL級邏輯鎖定技術 20

圖10 主要控制安全VA處理器的FSM 22

圖11 建議的VA處理器的佈局 26

圖12 平均預測速率作為第1層中鎖定技術的密鑰大小的函數 28

圖13 不同預測率操縱鎖定技術的執行時間 29

**表目錄**

表1 該工作的貢獻 6

表2 擬議的防禦層實現的安全目標 16

表3 ECG信號處理的性能評估 25

表4 安全VA處理器設計指標 26

表5 （安全）VA處理器硬體與先前實現設計的比較 27

表6 與單個防禦層的基本（無安全）設計相比 29

1. **緒論**

**1.1 物聯網和醫療保健**

　　電子和無線通信技術的發展催生了物聯網的時代[1]。由大量簡單互連組件組成，這些組件採用大規模通信來增強彼此的功能，支持物聯網的設備和系統可在醫療保健、能建築和智能交通系統中找到應用[2]。在醫療保健領域，正在部署數百萬個支持物聯網的植入式醫療設備（Implantable Medical Devices, IMD）[3]和可穿戴式設備[4]，其範圍從心臟除顫器和胰島素泵[5]到心電圖處理器[6]和健身追踪器[7]。通常包括傳感模塊、通信模塊以及應用模塊，支持物聯網的解決方案極大地幫助改善患者護理，提高整體生活質量。這些集成平台允許對健康資料進行連續聚合和智能挖掘/預處理，這些資料可以基於某些事件的檢測定期或明智地通過網絡傳輸到醫療機構以進行進一步評估。依靠電池/採集電源和持續監控操作延長使用壽命，對IMD和可穿戴式設備施加了嚴格的功耗限制。因此，能量效率是這些裝置中的主要問題。

**1.2 可穿戴/植入設備的安全挑戰**

　　在過去的十年中，生物醫學設備的安全性受到了極大的關注。在美國食品藥品監督管理局(Food and Drug Administration, FDA)批准的植入式設備[8]以及流行的健身追踪設備中已經證明了嚴重到危及生命的網絡攻擊，例如，Halperin 等。證明了心臟除顫器/心臟起搏器如何被竊聽和重新配置以對患者造成嚴重的電擊。大多數現有攻擊利用遙測/無線通信接口來提取敏感信息，例如設備識別碼和設備的增益控制。

　　(1)遙測對策：傳統的生物醫學設備防禦機制旨在實現安全的無線通信，主要側重於開發認證和加密算法和協議[9] - [11]。使用ECG或EEG等信號開發生物識別解決方案的趨勢越來越明顯[12][13]。然而，大多數認證方案採用計算複雜的算法，例如需要大量計算資源的大型神經網絡和支持向量機等，因此，不能實現為成本有效的集成（芯片上）解決方案。而且，這些解決方案僅解決整個生物醫​​學設備安全難題的一個方面。這些解決方案天真地假設底層硬體值得信賴，並忽略了新興的基於硬體的攻擊[14][15]。

　　(2)基於硬體的攻擊：由於全球化的IC供應鏈，出現了各種基於硬體的攻擊。在當今的橫向業務模型中，芯片可以在不同的國家進行設計、製造、封裝、測試和部署。大量（潛在的流氓）實體（如代工廠、測試設施、裝配廠、最終用戶）現在可以訪問芯片，擴大攻擊面。硬體特洛伊木馬形式的隱形惡意後門電路可以在製造/測試/組裝階段插入生物醫學芯片[16]。通過稍後觸發特洛伊木馬，攻擊者可能會洩漏敏感的患者信息。攻擊者甚至可以控制生物醫學設備並破壞其功能，例如，停止胰島素泵，改變除顫器中的電脈衝強度，或操縱ECG處理器的輸出。

　　類似於假冒藥物的威脅[17]，新出現的威脅是假冒生物醫學電子產品[18][19]，它可能危及患者的健康以及設計/製造公司的聲譽。某些假冒產品依賴於IC的逆向工程，其涉及拆包、去層、層成像和圖像註釋以提取門級網表。逆向工程也會導致IP盜版問題，因為知識產權所有者在做出重大努力後開發的有價值的設計IP可能會被盜版和克隆。盜版也可能發生在一家代工廠，該代工廠在成本略有增加的情況下建立額外的芯片並在黑市上銷售。IC供應鏈攻擊如圖1所示



圖1　IC設計流程中不同階段的新安全威脅。

　　硬體設計信任方法：阻止上述IC供應鏈攻擊，信任設計（Design-For-Trust, DfTr）方法，如邏輯鎖定[20] - [22]，IC偽裝[23]和分割製造[24]已經開發出來。在各種DfTr方法中，邏輯鎖定是最通用的方法，因為它可以防止不受信任的代工廠設施以及最終用戶攻擊。邏輯鎖定使用密鑰鎖定設計;如果沒有將正確的密鑰加載到芯片上（稱為激活），芯片就不會產生正確的輸出。它可以阻止盜版/逆向工程攻擊，同時提供抵禦硬體特洛伊木馬插入的彈性。已經為通用IC開發了現有的DfTr技術，並且在專用集成電路的背景下沒有研究機會和挑戰。

**1.3 威脅模型**

　　基於之前的討論，我們描述了可穿戴/可植入生物醫學設備的威脅模型，這是本文的重點。

　　誰是攻擊者？我們假設攻擊者可能是IC供應​​鏈中任何地方的流氓代理，包括不受信任的代工廠，測試或組裝工具。從生物醫學設備的角度來看，攻擊者可以是可以訪問激活的生物醫學芯片的最終用戶。攻擊者可能是不受信任的醫務人員，可以訪問患者攜帶的設備。

　　攻擊者可以獲得的資產？我們假設攻擊者可以訪問反向工程網表和功能芯片。網表可以通過逆向工程或盜版獲得。功能芯片可以從市場上合法購買，或者從攜帶它的患者獲得（借用或甚至被盜）。

　　攻擊者的目標。攻擊者希望實現以下一個或多個惡意/非法目標：1）對處理器網表進行反向工程以確定設計/演算法細節，2）盜用/過度構建生物醫學芯片，3）插入硬體特洛伊木馬以洩露私人資料或造成傷害，4）製造生物醫學設備的假冒複製品。

**1.4 目標：整體一體化**

　　從之前的討論可以看出，存在獨立的，孤立的解決方案，可以在個人基礎上解決物聯網的能效和安全挑戰。這些解決方案包括低功耗ECG處理器[25]，安全通信協議，信任設計解決方案和生物認證解決方案。每個解決方案都側重於特定挑戰，而不是解決其他問題。通常，設計工程師專注於低功耗和高性能的實現。安全性通常是經過深思熟慮的，現有的安全解決方案不適用於低系統的系統單晶片（System-on-Chips, SoC）。因此，必須研究以協同方式共同應對多種挑戰的整體解決方案，以開發安全且節能的片上系統。

　　本文重點介紹為生物醫學應用開發低功耗，安全的物聯網平台的方法。作為案例研究，我們開發了一種用於心室心律失常（Ventricular Arrhythmia, VA）預測的物聯網平台。VA是一種異常的心電圖節律，除非在幾秒鐘內治療，否則造成心髒病患者猝死的75％-85％[26]。VA事件包括心室心動過速（Ventricular Tachycardia, VT）或心室顫動（Ventricular Fibrillation, VF）。擬議的完全集成的VA處理器/ SoC旨在預測發病前3小時的VT / VF事件。通過預先預測這些事件，有足夠的時間提醒患者並為他們提供所需的醫療護理。圖2說明了所提出的VA處理器的使用。在片上收集和處理ECG資料，並且僅通過中間“工程師”設備將相關特徵發送到醫療機構。



圖2　可佩戴的VA SoC處理和分析ECG資料。當預測到異常VA事件時，僅將計算的特徵發送給醫生。

**1.5 建議的VA處理器**

　　VA處理器的主要輸入是數字化ECG信號，輸出是單比特預測類C代表正常/異常的心血管事件。SoC使用從VA開始之後的ECG段提取的特徵來訓練可以區分正常和異常病例的分類器。訓練基於離線計算參數，這些參數通過輸入SPI接口提供給設計。為了訓練和驗證我們的設計，我們從美國心臟協會（American Heart Association, AHA）獲得了一個資料庫，其中包括3個小時的記錄患有VT / VF病症的患者;在處理大約10次（大約10秒）後，我們的發動機能夠以超過86％的準確度預測VT / VF狀態。此外，我們已經對MIT Physionet資料庫中針對VT / VF病情患者的16個記錄進行了驗證。即使這些錄音的長度在20-30分鐘範圍內，我們的引擎也能夠對這些錄音進行操作。比較的基準是我們以前的VA處理器架構。我們設想VA處理器是可植入/可穿戴醫療設備的一部分。此外，該裝置可以使用從人體收穫的能量來供電[27]。

　　在本文中，我們使用65nm低功率增強（Low Power EnhancedL, LPe）技術中的專用集成電路（Application Specific Integrated Circuits, ASIC）設計流程來實現所提出的VA處理器。建議的設計具有以下特點：

1. 我們提出了VA預測中的算法增強，這導致架構改變（RAM大小和時鐘速度的降低），與現有技術相比，除了16.0％的面積減少之外，功率降低62.2％。
2. 我們識別VA處理器中的安全關鍵組件，並使用信任設計技術（邏輯鎖定）保護這些組件。
3. 我們提出了一種分層安全架構，每層都有特定的保護目標，從而實現成本安全性權衡。
4. 我們開發了ECG密鑰生成區塊，使用ECG信號提取唯一密鑰。通過將ECG密鑰與現有的信任設計解決方案相集成，該建議平台還可以在硬體級別提供保護，從而挫敗逆向工程和偽造等硬體安全威脅。ECG生成的密鑰使得能夠使用不同的密鑰解鎖每個VA處理器芯片。
5. 通過有效的資源共享，我們以最小開銷實現密鑰生成塊，僅佔2.7％的面積，0.2％的功率和零延遲。
6. 安全的VA處理器與建議的低功耗VA處理器相比，具有9.5％的低開銷和0.7％的功率。性能沒有影響。

　　表一介紹了這項工作的主要貢獻。

表1　該工作的貢獻。

|  |  |  |  |
| --- | --- | --- | --- |
| 序號 | 模組 | 目標 | 貢獻 |
| 1 | VA處理器 | 預先提前三小時預測VA事件的發生 | 所提出的架構直接處理輸入的ECG信號。與基線解決方案相比，功率降低了62.2％，面積降低了16.0％。 |
| 2 | 邏輯鎖定電路 | 防止IP盜版，逆向工程和修改 | 識別處理器中的安全關鍵組件並開發多層安全解決方案 |
| 3 | ECG密鑰產生器 | 使用ECG信號生成芯片專用密鑰 | 重新使用VA處理器組件進行密鑰生成，減少實現開銷。 |

　　雖然我們在本文中使用了特定的案例研究，但提出的方法是通用的，可用於其他類似的資源約束和安全關鍵的生物醫學應用。最重要的是，這項工作闡明了：

1. 通過將關鍵算法增強功能反映到架構改進中，可以使給定設計如何實現超低功耗。
2. 如何在給定設計的應用程序上下文中識別的安全目標可以轉換為包含在設計中的安全功能。
3. **背景和相關工作**

**2.1 以前關於ECG處理器的工作**

　　在[28]中提出了包括三個階段的ECG處理器，即預處理，特徵提取和分類。實現了基於四級矢量[29]的算法來執行這三個階段。此外，這些功能都是流水線的，以提高硬體利用率並降低整體功耗。此外，採用時鐘門控和電壓調節來進一步降低能量耗散。ECG處理器是用0.18μm和消費6μW 在1.8V和1.26μW。在[30]中提出了另一種ECG分類系統。整個系統由三個獨立的芯片實現。第一個芯片包含體端電路，它是基於高通調製器的生物信號處理器（High-Pass Sigma Delta Modulator-Based Biosignal Processor, HPSDM-BSP）和開關鍵控發送器。第二個芯片，即接收端，有接收器和數位訊號處理（Digital Signal Processing, DSP）單元。最後一個芯片是分類器。DSP單元採用離散小波變換進行ECG特徵提取和分類。該芯片是在上面製造的0.18μm CMOS技術消耗了總功率 5.967μW僅在1.2V 時為DSP單元。節拍檢測和心電圖分類的準確率分別為99.44％和97.25％。報告的結果僅用於檢測VA，而不是其預測。

**2.2 以前的硬體安全工作：邏輯鎖定**

　　據我們所知，以前的工作沒有考慮保護生物醫學SoC的底層硬體。現有的努力僅側重於安全通信。由於我們將邏輯鎖定作為基於硬體的防禦的基本部分，因此我們將本節中的調查限制為邏輯鎖定。有關其他DfTr技術的詳細描述，感興趣的讀者可以參考一般調查論文[31]。

　　邏輯鎖定是一種DfTr技術，旨在通過使用密鑰鎖定設計來防禦IP盜版，過度構建，硬體特洛伊木馬和逆向工程攻擊。為了啟用芯片鎖定功能，將額外的邏輯，例如，一組稱為關鍵門的XOR / XNOR添加到原始網表中，從而產生鎖定的網表。鎖定的網表通過不受信任的設計/製造階段，如圖3所示。如果不知道密鑰，鎖定的網表就無用了。

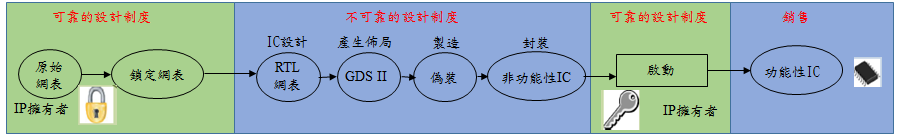


圖3　IC設計流程的邏輯鎖定。該設計在不受信任設計體系中處於鎖定狀態。

　　範例：圖4a顯示了一個示例多數電路網表，圖4b顯示了具有三個XOR / XNOR鍵門的鎖定版本。每個鍵門的一個輸入由原始設計中的導線驅動，而另一個輸入稱為鍵輸入由存儲在防篡改存儲器中的鍵位驅動。網表中的逆變器可以被氣泡推動以增加混淆複雜度，如圖4c所示。鎖定的IC或鎖定的網表將無法生成正確的輸出，除非使用正確的密鑰激活它。考慮圖4b中的鎖定電路。當應用正確的鍵110時，輸出正確和 輸入模式000獲得= 0。但是，對於相同的輸入模式，輸出不正確 和 對於任何不正確的鍵值產生= 1。

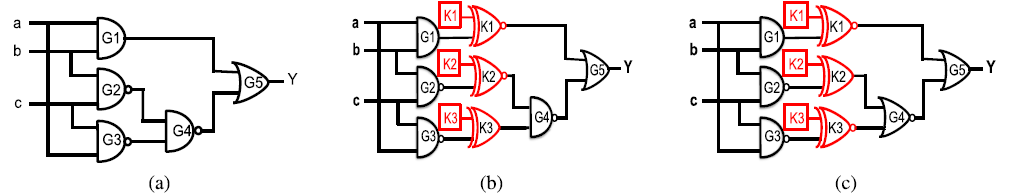


圖4　使用XOR / XNOR門進行邏輯鎖定。(a)示例電路：三個輸入中的大多數。(b)使用XOR / XNOR鍵門鎖定電路。正確的鍵值是110. (c)鎖定電路，其中逆變器吸收了關鍵門。正確的鍵值仍然是110。

**邏輯鎖定如何解決硬體信任問題？**即使逆向工程攻擊者竊取鎖定的網表或通過反向工程IC獲得它，如果不知道正確的密鑰，網表將毫無用處。同樣，邏輯鎖定阻止了盜版和基於克隆的偽造攻擊。邏輯鎖定還阻礙了惡意代工廠的過度構建，因為在不知道密鑰的情況下，製造的芯片將無法正常工作。邏輯鎖定試圖通過使攻擊者更難以識別插入特洛伊木馬的安全位置來防止將木馬插入網表。關鍵門以攻擊者未知的方式改變信號的轉移概率[32]。

　　邏輯鎖定的類型：

　　(1)隨機邏輯鎖定：隨機邏輯鎖定（Random Logic Locking, RLL）通過在網表中的隨機位置插入XOR鍵門來鎖定設計網表。圖4b顯示了使用RLL用三個鍵門K1，K2和K3鎖定的網表示例。

　　(2)基於故障分析的邏輯鎖定：基於故障分析的邏輯鎖定（Fault analysis based Logic Locking, FLL）旨在防止IC的黑盒使用。在隨機邏輯鎖定中，即使不正確的鍵也可能導致某些輸入模式的正確輸出。基於故障分析的邏輯鎖定可確保在使用不正確的密鑰時輸出位最大損壞。輸出損壞是根據正確輸出和不正確輸出之間的漢明距離百分比來衡量的，這是在應用不正確的密鑰時獲得的。

　　(3)強大的邏輯鎖定：強邏輯鎖定以最大化關鍵門之間的干擾的方式插入關鍵門，並且在個體基礎上防止關鍵位的敏感化。隨著關鍵門之間干擾的增加，攻擊者被迫強制指數增加數量的關鍵組合。

　　(4)SARLock：SAT攻擊抵抗邏輯鎖定：SAT攻擊[33]是對邏輯鎖定技術最強大的攻擊之一。該攻擊基於使用專門的區分輸入模式（Discriminating Input Patterns, DIP）消除不正確密鑰的概念，逐漸識別密鑰。SARLock[34]通過確保DIP的有效性受到限制來抵禦SAT攻擊; SARLock構造確保每個DIP最多可以消除一個不正確的密鑰，從而導致攻擊的指數執行時間。要真正有效，SARLock必須與另一種邏輯鎖定技術相結合，如FLL或RLL。在本文中，我們將SARLock視為額外的安全層。

**2.3 關於ECG密鑰生成的先前工作**

　　密碼算法是任何安全通信基礎設施的支柱，它依賴於密鑰。通常使用偽隨機數生成器（Pseudo-Random Number Generators, PRNG）生成這些密鑰。為了滿足美國國家標準暨技術研究院(National Institute of Standards and Technology, NIST)標準所規定的所需隨機性屬性，PRNG在隨機種子上運行計算複雜的處理算法，使得它們對於電池供電的可穿戴設備而言是不切實際的。對於這樣的設備，可以使用諸如ECG[35][36]的生理信號生成秘密密鑰。ECG信號隨著時間的推移不可再現，並且難以用於人的直接生物識別認證。然而，基於ECG信號生成的二進制序列（密鑰）表現出良好的隨機性，甚至可以滿足NIST標準。早期基於ECG的密鑰生成方法使用脈衝間間隔（Inter-Pulse Interval, IPI）也稱為RR間隔，參見圖5[37]以及可能具有高延遲的糾錯電路（Error Correction Circuitry, ECC）。然而，最近基於ECG的密鑰生成已經通過直接量化RR和其他ECG特徵而沒有任何ECC來實現，同時通過NIST統計測試。

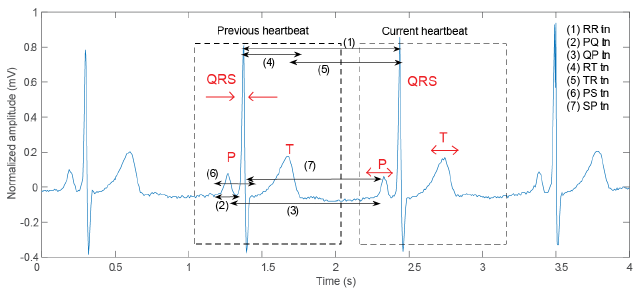


圖5　帶註釋ECG波形，突出顯示ECG波分量和為ECG分類器提取的特徵。

1. **VA處理器架構**

　　基線VA處理器包括三個主要階段：ECG預處理，特徵提取和分類，如圖6所示。在ECG預處理階段，提取所有ECG波特徵，例如QRS波群，T波和P波。在ECG描繪之前，執行濾波是因為ECG可能被基線漂移，電力線干擾和高頻噪聲破壞。過濾後，基於Pan和Tompkins技術進行QRS檢測[38]。與QRS峰值檢測一起，還描繪了QRS起始和偏移。最後，描繪T波和P波，並提取相應的基準點（P開始，P峰，P偏移，T開始，T峰和T偏移）。

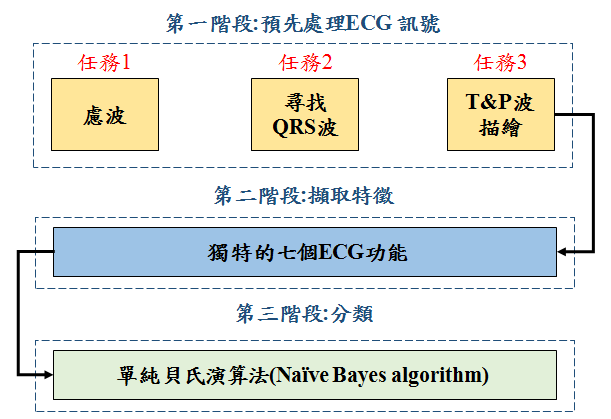


圖6　心室心律失常預測系統示意圖。

在這項工作中，進行了三項主要修改以降低功耗：1）消除QRS檢測中的SRAM模塊，從而將RAM要求從8KB降低到4KB。2）將工作頻率降低到250 Hz，等於ECG採樣頻率。3）使用高閾值電壓（HVT）電池來降低洩漏功率。優化的細節將在以下小節中討論。

**3.1 心電圖預處理**

　　ECG代表心臟的電活動，其特徵在於不同的波分量。圖5顯示了各種ECG特徵，即QRS波群，T波和P波。描繪過程的任務是準確地識別這些波的起始，峰值和偏移。

　　在基線架構中，對存儲在SRAM中的樣本執行QRS檢測。但是，在更新的架構中，QRS峰值直接從新樣本中檢測到，無需存儲轉換後的樣本。這種看似微小的改進實際上導致面積和功耗的大幅降低。如圖7所示，移動積分器的輸出被直接相比，R-峰值檢測模塊中的閾值。即使在時鐘頻率等於採樣頻率的情況下，這種優化也使系統能夠實現實時操作。其他特徵，如QRS的起始/偏移，以及T波和P波的起始/峰值/偏移使用存儲在存儲器中的過濾樣本計算。在架構中使用兩個記憶體區塊，它們可替代地用於存儲新樣本和同時讀取/處理。無論何時從記憶體1進行描繪，新的濾波信號都存儲在記憶體2中，反之亦然。注意，當檢測到新的QRS峰值時，執行兩個SRAM的描繪和切換功能（讀/寫）。

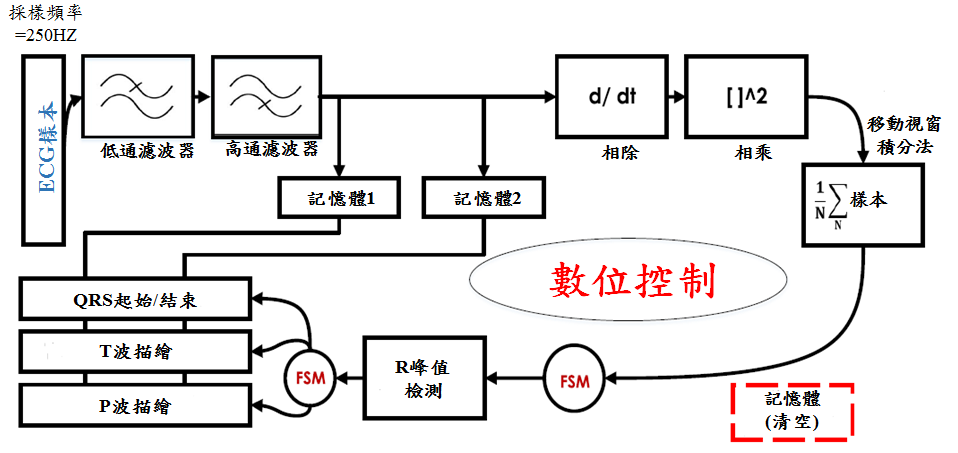


圖7　預處理階段的流程圖，包含過濾，QRS檢測和P和T波描繪。與基線8KB相比，所提出的架構中僅需要4KB RAM。所提出的架構不需要記憶體來存儲變換的樣本。

**3.2 特徵提取階段**

　　此階段提取分類器使用的功能。我們首先確定最能捕捉心室心律失常特徵的獨特心電圖特徵集。這些功能包括：RR，PQ，QP，RT，TR，PS和SP間隔。圖5顯示了代表性ECG記錄上的這些間隔。值得一提的是，這些特徵是從兩個連續的心跳中提取的，與其他獨立處理每個心跳的方法不同。利用兩個連續的心跳可以更準確地預測VA 。

**3.3 分類階段**

　　分類器的目的是基於上述特徵預測VA的存在。由於我們的系統旨在實現超低功耗，因此只能提供需要最少硬體資源的分類器架構。考慮到這一點，選擇了樸素貝葉斯分類器。樸素貝葉斯分類器是一種線性分類器，易於構建，無需複雜的迭代參數估計。它假設特徵向量之間存在天真且強烈的獨立分佈，並且滿足了這一假設，因為所有提取的ECG特徵都從頭開始獨立分析和評估。

　　圖5顯示了心電圖記錄中的六個間隔。這些特徵被徹底研究為VT / VF條件的最佳指標，對於我們研究的VT / VF記錄資料庫以及許多正常ECG記錄，這些特徵使得能夠使用貝葉斯分類器。主要地，信號的高質量差異使得能夠成功地使用線性分類器來進行決策制定。

1. **安全VA處理器**

**4.1 安全目標**

　　如果不採用任何安全措施，建議的VA處理器仍然容易受到可能對患者的安全，福祉和隱私構成嚴重危險的攻擊。此外，從設計、製造和分銷處理器的公司的角度來看，安全性也是一個重要的問題。基於威脅模型和預期的應用程序，我們考慮VA處理器的以下安全目標：

1. 保護VA處理器實施和秘密設計參數免受盜版/逆向工程攻擊。
2. 防止在處理器中插入惡意木馬。
3. 防止使用處理器的非真實（偽造）複製品;防止黑盒使用。
4. 使用ECG信號生成唯一密鑰，並使用相同的芯片專用密鑰來保護通信接口並阻止基於硬體的攻擊。
5. 保護用於鎖定設計的密鑰。

　　基於這些安全目標，我們開發了一個多層防禦方案，包括以下四個層次：

1. 預測率操縱。
2. SAT攻擊彈性。
3. 拒絕服務。
4. ECG密鑰生成。

　　分層方法提供了根據安全規範包含/排除安全組件的靈活性，從而在成本和安全性之間進行權衡。第一防禦層（稱為預測速率操縱）集成了邏輯鎖定，以在應用不正確的密鑰時破壞VA處理器的功能。這實現了多個目標;秘密密鑰值應該是已知的（1）以完全理解設計實現細節和（2）激活芯片並使其起作用（恢復預測精度），結果實現了O1和O2目標。第二層提供抵禦新興SAT攻擊的彈性 關於邏輯鎖定。第三層通過將處理器FSM鎖定在中間階段來提供對黑客攻擊的保護，黑客攻擊可以控制處理器，從而導致拒絕服務。由於邏輯鎖定在FSM內是隔離的，因此只能實現O3目標。第四層包括密鑰生成塊，其從ECG信號中提取芯片專用密鑰。我們相信，隨著使用ECG成熟的生物識別認證的研究，該層可以包含患者特定的密鑰。由於基於ECG的密鑰（以及其他基於ECG的認證方案）的可重複性較差，我們僅限於使用芯片專用密鑰。表2顯示了各個層實現的目標。

表2　擬議的防禦層實現的安全目標。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 層/目標 | L1 | L2 | L3 | L4 |
| O1 | 🗸 |  |  |  |
| O2 | 🗸 |  |  |  |
| O3 |  |  | 🗸 |  |
| O4 |  |  |  | 🗸 |
| O5 |  | 🗸 |  |  |

**4.2 識別要保護的處理器區塊**

　　雖然可以保護整個處理器，但是由此產生的開銷將是令人望而卻步的。此外，處理器中的某些區塊可能不是安全關鍵的（在所述威脅模型下）。因此，我們對VA處理器中的各種區塊進行分析，並確定那些對安全性至關重要的塊。時鐘分配單元、電源管理單元、I/O接口和存儲器接口都是標準的，眾所周知的電路，其設計/優化以提高性能。但是，這些區塊不包含需要保護的秘密。與上述區塊類似，ECG預處理和特徵提取器區塊也實現了眾所周知的（儘管是優化的）算法。想要盜版或克隆VA處理器的攻擊者可以使用現有的已知算法來提取相同的功能集，而不是將精力投入到對芯片進行逆向工程的費力過程中。然而，攻擊者肯定感興趣的是參數，例如從私人患者資料中學習的不同參數的平均值和標準偏差。因此，我們將“ECG分類器”識別為VA處理器中最安全關鍵的組件。為了防止逆向工程和其他攻擊，我們探索了兩種不同的邏輯鎖定技術。為了保護分類器參數，我們提出了基於設計參數的邏輯鎖定（Design Parameter based Logic Locking, DPLL）。此外，為了保護處理器的黑盒使用，我們還開發了預測率邏輯鎖定（Prediction Rate Logic Locking, PRLL）。這些技術在後面章節中進一步描述。

**4.3 安全VA處理器架構**

　　圖8顯示了所提出的安全性心室心律失常預測處理器的總體結構。增加了兩個模塊，ECG鍵發生器和防篡改存儲器，以實現芯片上安全功能。此外，修改了兩個區塊，即主FSM和ECG分類器（以橙色突出顯示）。使用邏輯鎖定技術中的一種（或組合）來鎖定ECG分類器區塊，並將其稱為鎖定ECG分類器。只有為區塊提供了正確的解鎖密鑰，該區塊才能正常工作。ECG密鑰生成器使用來自患者的ECG信號來提取唯一的ECG密鑰對於每個部署的芯片，從而啟用芯片專用密鑰。基於ECG鍵和解鎖鍵的值，生成芯片專用可編程密鑰並將其加載到防篡改存儲器上。該架構允許使用不同的密鑰解鎖每個芯片，避免了與患者或醫務人員共享公共密鑰的問題。此外，ECG生成的密鑰可以進一步用於加密遙測接口上的通信。VA處理器還可以是更大平台的一部分，該平台包括諸如心臟除顫器之類的IMD，其向患者提供受控電擊。在這種情況下，ECG發生器可以進一步用於通過使用心臟到心臟協議來實現對醫務人員的緊急訪問。

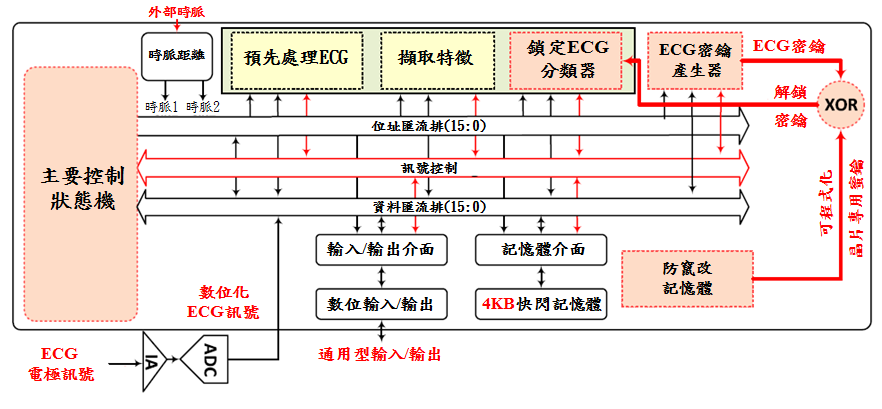


圖8　提出的安全性心室心律失常預測處理器的結構。與安全相關的塊以橙色突出顯示，帶有虛線邊框。

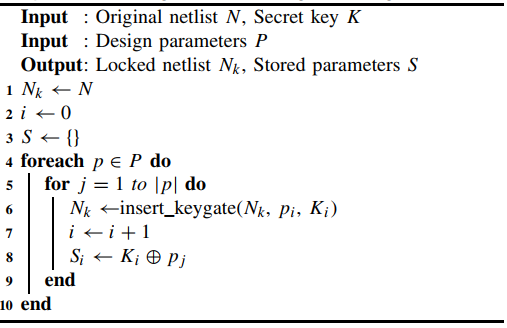
**4.4 第1層：預測率操縱**

　　我們開發了兩種邏輯鎖定技術，DPLL和PRLL，目的是操縱預測率以便為攻擊者產生最大的模糊性。

　　(1)設計參數保護邏輯鎖定：VA處理器的主要部分以及安全關鍵分類器由眾所周知的標準組件組成。設計人員的關鍵資產只是從ECG訓練資料中學到的秘密設計參數，並且在VA事件的芯片上分類中用作正常/異常。感興趣的參數包括正常/異常分佈的“平均值”和“標準偏差”。想要克隆/竊取設計的攻擊者只需要提取這些設計秘密。讓這些秘密參數不受保護會使實現暴露在之前章節中討論的基於硬體的攻擊中。我們建議用XOR鍵門鎖定設計者提供的設計秘密。在DPLL中，而不是使用秘密參數的實際值 ，我們存儲修改後的值 。只有激活芯片後，正確的密鑰才能恢復設計密鑰的正確值。在行使不正確的鍵值時，攻擊者將觀察到不正確的預測輸出。

　　如演算法1中所述，設計參數是DPLL算法的輸入;算法生成存儲的參數S。該算法為每個位插入一個鍵門 在設計參數中。DPLL可以在寄存器傳輸級（Register Transfer Level, RTL）實現。

演算法1　設計參數邏輯鎖定。



　　(2)基於預測速率的邏輯鎖定：邏輯鎖定必須確保錯誤的鍵值導致輸出錯誤。對於VA處理器，最終輸出是表示心室心律失常的預測（是/否決​​定）的一位信號預測類。預測率描述VA處理器正確預測心律失常事件的正確/錯誤鍵的時間百分比。在DPLL中，不正確的密鑰可能並不總是產生不正確的輸出;對於某些不正確的鍵值，預測率可能很高。為了克服這個限制，我們提出了基於預測速率的PRLL。在PRLL中，插入關鍵門以產生最差的預測速率，即最接近50％的預測速率。該預測速率最大化了攻擊者的模糊性，因為VA處理器的輸出似乎隨機行為。預測率為0％意味著攻擊者沒有歧義，因為他/她可以簡單地反轉輸出。

　　PRLL可以在門級或RT級實現。RT級實現在插入關鍵門之後為設計者節省了重新合成網表的額外步驟。由於平方運算放大了輸入中的誤差（對於不正確的鍵），我們將關鍵門插入正方形區塊的輸入端，如圖9所示。

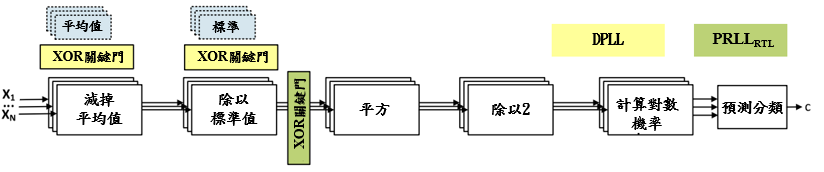
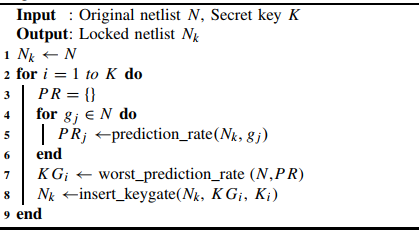


圖9　抽象表示RTL級邏輯鎖定技術：DPLL和，在安全關鍵ECG分類器區塊上實現。該塊並行處理計算的特徵，並聚合正常/異常類概率以計算最終預測c輸出。在DPLL中，關鍵門插入源自參數的選定導線（以淺藍色突出顯示，並在訓練階段學習）。在中，鍵門插入“正方形”區塊的輸入端。

　　邏輯層實現PRLL從FLL改編而來。必須注意的是，和PRLL層指的是具有相同目標的兩種不同的邏輯鎖定技術/算法：對不正確的鍵值實現50％的預測。前者是在RT級操作的技術，而後者是在合成門級網表上操作。與相比，PRLL層的計算複雜度更高。我們詳細說明了結果部分中和之間的選擇。

　　演算法2描述了PRLL層算法。在算法的每次迭代中，將關鍵門插入產生最差（最接近50％）預測率的位置。通過模擬1000個隨機輸入模式來計算用於在層的輸出處插入關鍵門的預測率。算法的複雜性在於，代表密鑰的大小，是網表中N的層數。

演算法2　基於預測率的邏輯鎖定。



**4.5 第2層：SAT攻擊彈性**

　　最新的逆向工程攻擊利用布爾可滿足性（Satisfiability, SAT）求解器。為了阻止SAT攻擊，我們將SARLock作為VA處理器的附加安全層。我們將SARLock與鎖定的ECG分類器以及PRLL和DPLL中的一個集成在一起。

**4.6 第3層：拒絕服務（Denial of Service, DSLL）**

　　通過將有限狀態機鎖定在VA處理器中，我們可以保證處理器將卡在中間階段並且永遠不會產生正確的輸出，除非在片上加載正確的密鑰。因此，防止了VA處理器的非法/未授權使用。我們使用RLL任意鎖定視窗分界狀態並且觀察到沒有正確的密鑰，處理器不會進入後續階段。雖然DSLL阻止對鎖定的FSM的各種攻擊並確保拒絕服務，但它只能與其他安全層一起使用。DSLL阻止對試圖控制設備的設備進行主動黑客攻擊。DSLL還表明，硬體級安全技術可以幫助滿足整體應用程序級別的安全性要求，從而禁用未授權代理的控制/訪問。

**4.7 第4層：ECG密鑰生成**

　　為了向使用中的每個VA處理器分配芯片特定的唯一密鑰，我們使用人的ECG信號為每個芯片生成隨機密鑰。相同的密鑰也可用於加密處理器和“編程器”設備之間的通信。每個芯片的唯一密鑰還可確保即使其中一個芯片受損，其他芯片也不會受到影響。

　　對於輕量且可靠的ECG密鑰生成，我們採用中提出的方法，並使用特徵提取階段生成的七個特徵直接用於ECG密鑰生成。提取的七個特徵各為11位。我們連接這些功能以生成77位密鑰。使用所選特徵的線性組合，我們構造一個128位密鑰，用於解鎖處理器。ECG密鑰生成需要對VA處理器進行最少的修改。通過復用相同的預處理和特徵提取邏輯，我們避免了額外的面積，功耗和延遲開銷。VA處理器的主控制FSM略有修改。附加的ECG密鑰生成狀態被添加到處理器的主FSM，如圖10所示。在這種狀態下，從患者記錄ECG信號，並且基於從ECG信號提取的特徵生成唯一的ECG密鑰。

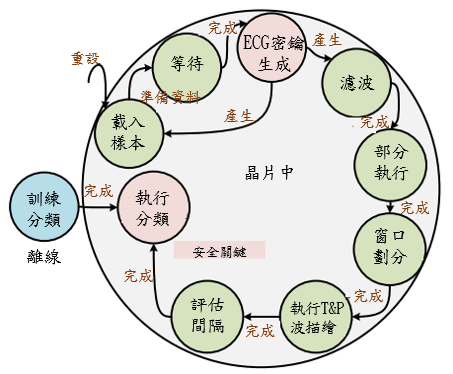


圖10　主要控制安全VA處理器的FSM。與安全相關的狀態以紅色陰影顯示。

　　VA處理器的可靠操作取決於ECG生成的密鑰的可靠性。如果與密鑰生成，存儲或檢索相關聯的邏輯（讀取生成的密鑰值）表現出錯誤的操作;VA處理器輸出不正確，導致錯誤或抑制警報。被抑制的警報，即異常VA事件被報告為正常的情況，由於它們可能危及患者的生命，因此更受關注。可以利用諸如糾錯碼（Error Correcting Codes, ECC）和三重模塊冗餘（Triple Module Redundancy, TMR）的各種可靠性增強技術來增強ECG密鑰生成模塊的可靠性。

**4.8 芯片專用密鑰生成**

　　根據以下協議，在將設備交給患者之前，在可信醫療機構生成ECG密鑰和每個芯片的可編程芯片專用密鑰KCS：

1. 芯片上電並監測患者的ECG信號。 基於ECG信號，在芯片上生成並存儲在非易失性存儲器中。
2. 基於從芯片讀取的值，的值計算如下：，是VA處理器的解鎖鑰匙，只有授權人員才知道。
3. 通過將加載到一次性可編程防篡改存儲器上來激活芯片。 然後將激活的裝置移交給患者。 使用和解鎖VA處理器芯片如圖8所示。
4. **實驗與結果**

**5.1 實驗框架**

　　我們進行MATLAB模擬，然後使用Modelsim和Synopsys工具進行廣泛的Verilog模擬，以驗證設計的功能。端到端系統使用Verilog-HDL設計，並創建了一個測試平台，通過對輸入資料建模來模擬它。輸入信號是以250Hz採樣的數位化ECG資料。此外，驗證處理器在不同的時鐘頻率下工作，並且我們報告250Hz的工作頻率的性能，這是基於採樣率的最低可能頻率。

　　Synopsys最先進的設計工具用於合成、佈置和佈線設計，獲得設計區域並估算功耗。對於單獨的邏輯鎖定技術，我們已經報告了使用Synopsis DC編譯器進行邏輯綜合後獲得的結果;我們使用了單元區域而不是門/單元數來計算區域開銷。另一方面，對於整個處理器，我們使用Synopsis IC Compiler報告了DRC-clean佈局的開銷。

　　我們使用Synopsys Formality驗證所提出的具有不同安全層的安全VA處理器的正確性，以及使用Modelsim進行廣泛的RT級和門級模擬。在驗證期間，秘密密鑰用作約束。RT級邏輯鎖定技術使用自定義Python腳本實現。HOPE故障模擬工具[39]用於在中查找關鍵門位置。所有模擬均在配備6核Intel Xeon W3690 CPU的服務器上運行，運行頻率為3.47GHz，內存為24GB。

**5.2 表現結果**

　　這項工作的研究資料集包括兩組;A組包括從PhysioNet NSRDB[40]獲得的一組5條單導聯正常ECG記錄，並以250Hz採樣。這些記錄沒有明顯的心律失常。B組共涉及6個單導聯逐拍註釋異常ECG記錄，伴有明顯的心室心律失常。這些記錄顯示出嚴重的異常，並從兩個來源獲得，包括美國心臟協會（American Heart Association, AHA）[41] 250Hz採樣記錄和MIT-BIH以360Hz採樣的記錄。所有選擇的ECG記錄都註釋為正常心跳，心室顫動的開始和結束，心動過速或撲動。此外，我們的分析在心室心律失常發作前使用了三秒鐘的窗口。通過在開始前幾秒移動窗口來執行分析，其中信號表現得非常正確，直到每個記錄的相關長度。通過這樣的分析，甚至可以提前三小時預測VT / VF發作。

　　在模型中模擬ECG資料後獲得的分類結果列於表3中。這些結果基於3秒處理窗口上的分類器輸出。

表3　ECG信號處理技術的性能評估：為建議和基線架構實現了相同的結果。

|  |  |
| --- | --- |
| 總結果 | 百分比(%) |
| 真陽(True Positive, TP) | 84.3 |
| 真陰(True Negative, TN) | 87.0 |
| 偽陰(False Negative, FN) | 15.7 |
| 偽陽(False Positive, FP) | 13.0 |

**5.3 ASIC設計**

　　VA處理器採用Verilog-HDL設計，佈局採用標準物理設計流程生成;使用GlobalFoundries 65nm LPe程式庫。我們使用Synopsys Design Compiler合成了設計，然後使用Synopsys ICC編譯器進行了平面規劃，放置和路由。我們提供的結果基於佈局後和芯片完成設計。由於我們的設計純粹是數字化的，因此在矽片後結果和佈局後設計之間預期非常高的相關性（在芯片設計行業中可接受的5％水平）是很自然的。圖11顯示了該設計的平面圖。已放置和佈線的VA處理器佔用空間尺寸為430μm通過218µm總利用率為85％。表4列出了設計結果。該設計佔據了核心總面積消耗了總的力量1.052μW頻率為250Hz。報告的實現使用8KB SRAM，QRS檢測器使用4KB，檢測其他功能使用4KB。在圖8所示的改進架構中，僅需要4KB SRAM來檢測QRS起始/偏移，T波和P波。從移動平均信號的輸出直接檢測QRS峰值。這種方案使總功率減少62.2％，面積減少16.0％。此外，這種新架構的工作頻率與採樣頻率相同。這是ECG處理器可以運行的最低頻率，以滿足實時要求。低頻運行也會降低動態功耗。

表4　安全VA處理器設計指標。

|  |  |
| --- | --- |
| 參數 | 數字 |
| 總面積 |  |
| 動力 |  |
| 洩漏功率 |  |
| 總電力 |  |
| 利用率 | 85% |

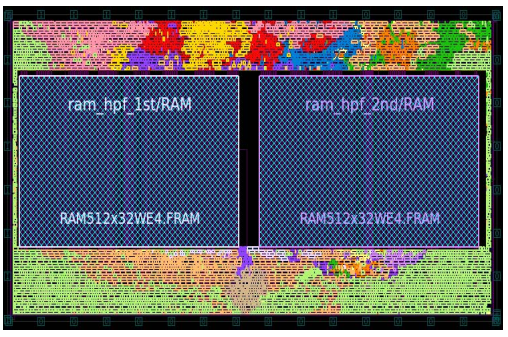


圖11　建議的VA處理器的佈局。

　　表5列出了所提出的VA處理器與現有ECG處理器的比較。所提出的架構基於從P波，T波和QRS波群提取的多個ECG特徵來執行預測;另一方面，先前的處理器 [42]僅基於RR間隔執行檢測。儘管報告中的功耗低於我們提出的處理器，由模擬模區塊控制，並且它僅執行無預測的心律失常分類。與和相比，所提出的VA處理器具有更低的功耗和面積。

表5　（安全）VA處理器硬體與先前實現設計的比較。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 參考 | 技術(μm) | 面積(mm2) | 功率(μW) | 電源電壓(V) | 頻率(KHz) | 檢測準確性(%) | 預測準確性(%) | 安全 |
| [28] | 0.180 | 2.250 | 1.260 | 0.7 | 1 | NA | NA | 不安全 |
| [30] | 0.180 | 2.465 | 5.967 | 1.2 | 0.12 | 97.25 | NA | 不安全 |
| [42] | 0.065 | 3.321 | 0.095 | 0.4 | 10 | NA | NA | 不安全 |
| **基線VA** | **0.065** | **0.112** | **2.780** | **1.2** | **10** | **NA** | **86** | **不安全** |
| **建議VA** | **0.065** | **0.094** | **1.052** | **1.2** | **0.25** | **NA** | **86** | **不安全** |
| **建議安全VA** | **0.065** | **0.103** | **1.059** | **1.2** | **0.25** | **NA** | **86** | **安全** |

**5.4 安全技術：鎖定對預測率的影響**

　　為了證明邏輯鎖定技術的有效性，我們將平均預測率報告為密鑰大小的函數。對於的每個值，生成1000個隨機密鑰值，並且監視處理器輸出以獲得多個ECG波形。預測率表示即使使用隨機密鑰的正確預測的百分比。如已經強調的那樣，期望50％的預測率。圖12顯示能夠僅使用十個關鍵門實現所需的50％預測率。相比之下，需要至少40個關鍵門。DPLL還需要大約40個關鍵門才能達到50％的預測率。然而，必須注意的是，對於，所有三種技術的行為是可比較的，並且可以選擇任何一種技術以滿足所需目標。因此，如果設計參數是要保護的最關鍵資產，則單獨使用DPLL可能就足夠了。否則或可能構成第一層防禦。

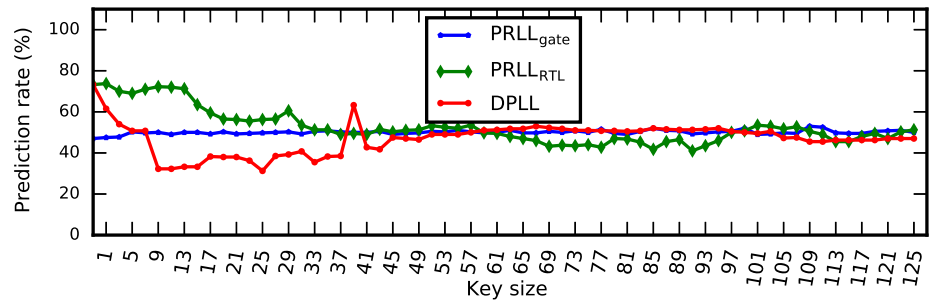


圖12　平均預測速率作為第1層中鎖定技術的密鑰大小的函數。對於多個ECG波形，在每個密鑰大小處執行1000個不正確的密鑰值，並報告平均預測速率。

　　請注意，使用SARLock的第二層的預測率將接近100％。SARLock服務於抵制基於SAT的攻擊的補充目標。無法報告第三層DSLL的預測速率，因為處理器隨後被鎖定在中間階段，並且從不生成最終輸出。

**5.5 安全技術：執行時間**

　　圖13顯示了作為第一安全層的替代方案所研究的三種邏輯鎖定技術的執行時間。可以注意到，RT級技術中每次迭代的執行時間約為一秒;因此，對於PRLL RTL和DPLL，可以在大約100秒內插入128個關鍵門。門級仿真在計算上是昂貴的。中單次迭代的執行時間約為一分半鐘;因此，插入128個關鍵門的總執行時間約為3小時。在插入關鍵門之後還需要額外的重新合成步驟。因此，在所提出的VA處理器的上下文中，採用RT級邏輯鎖定技術就足夠了，該技術可以在幾秒而不是幾小時內實現相同的安全目標，即所需的預測速率。

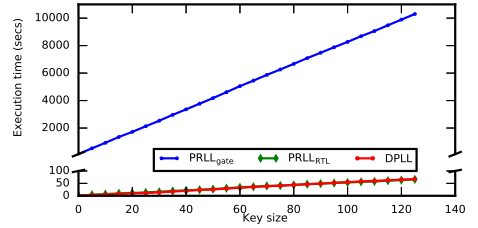


圖13　不同預測率操縱鎖定技術的執行時間。

**5.6 安全技術：面積，功率，延遲開銷**

　　必須滿足VA處理器的安全目標，而不會產生明顯的面積，功率和延遲開銷。表6報告了各個防禦層的開銷。VA處理器的性能並不重要，因為它的設計工作頻率為250Hz。我們以250Hz的目標頻率合成VA處理器，並報告鬆弛作為零延遲開銷。因此，對於所有防禦層，延遲開銷為零。

表6　與單個防禦層的基本（無安全）設計相比，安全SOC的面積，功率和延遲開銷。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 安全層 | 技術 | 面積(%) | 功率(%) | 延遲(%) |
| 第1層:預測率操縱 | PRLLRTL | 7.0 | 0.1 | 0 |
| PRLLgate | 0.9 | 0.1 | 0 |
| DPLL | 15.2 | 0.4 | 0 |
| 第2層:SAT彈性攻擊 | SARLock | 0.9 | 0.1 | 0 |
| 第3層:拒絕服務 | DSLL | 0.7 | 0.1 | 0 |
| 第4層:ECG密鑰生成 | - | 2.7 | 0.2 | 0 |

　　第一層可以觀察到，在預測速率操縱技術中，DPLL具有最高的區域開銷。如果沒有保護，設計參數是恆定的，可用於優化相關邏輯。但是，當參數被鎖定時，禁用優化和隨後的面積開銷減少。不安全VA處理器的單元面積約為，組合區佔總面積的21％。在DPLL鎖定電路中，插入了62.5％的附加組合單元，這使得組合單元面積從大約增加到，導致相對於VA處理器的總面積整體增加大約15％。相應的功率增加僅為0.4％，因為VA處理器的功耗主要由SRAM模塊的洩漏功率決定;SRAM模塊消耗的功率超過VA處理器總功耗的90％。

　　在PRLLRTL中，關鍵門插入正方形區塊的輸入端。我們觀察到，與DPLL類似，PRLLRTL也阻礙了相乘和DIV / 2區塊合成期間的優化。平均值的減法和除法通常會使輸出的最高有效位冗餘，從而導致面積減小。但是，當插入XOR / XNOR鍵門時，這種減少機會消失，因為正方形區塊的輸入也依賴於除主要輸入之外的鍵輸入。面積開銷增加7.0％;這不到DPLL增加的一半，DPLL鎖定了設計參數。PRLLgate另一方面，在門級網表上運行，該網表已經過優化，並且不會妨礙任何優化，與DPLL或PRLLRTL相反。PRLLgate只增加了128個XOR / XNOR鍵門，此外還有大約75個單元在重新合成過程中插入。每個插入單元的平均面積為，PRLLgate的整體面積增加約為0.9％。PRLLgate的功率開銷僅為0.1％。

　　考慮到功率和面積，PRLLgate是第1層最具成本效益的選擇。但是，這種技術的執行時間最長。如果關注執行時間，則設計者可以選擇PRLLRTL，而不會損失任何安全性（50％的錯誤鍵值預測率），代價是更高的面積和功率開銷。與PRLLgate中的關鍵門位置的算法選擇相比，關鍵門位置在PRLLRTL中相當臨時地選擇，遵循方塊放大注入誤差的直覺。PRLLRTL的更高開銷強調採用算法方法。

　　其他防禦層。後續防禦層的開銷甚至更低。例如，防禦層2,3,4的功率開銷分別為0.1％，0.1％和0.2％。第2層，SARLock，基本上包括一個128位相等比較器和一個XOR門。第3層DSLL使用隨機邏輯鎖定保護VA處理器中的FSM。第2層和第3層的面積開銷分別為0.9％和0.7％。第4層由密鑰生成區塊組成。一旦生成，芯片專用的ECG密鑰需要存儲器用於存儲，這會產生額外的面積和功率開銷。因此，與第二層和第三層相比，第四層的開銷是更高的2.7％面積和0.2％的功率開銷。全部四層（帶PRLL 門在安全VA處理器中採用選擇的第一層），總功率和麵積開銷分別為0.7％和9.5％。建議的安全VA處理器僅消耗，相比之下要低得多 對於基線處理器。表5列出了所提出的VA處理器（不安全和安全版本）與現有ECG處理器的比較。

1. **討論和未來的工作**

　　本文旨在引起學術界對物聯網平台硬體安全的重要性的關注，以及對作為安全信任根的硬體的盲目信任如何導致潛在的災難性後果。本文的貢獻在於開發一種方法，用於輕量級集成獨立的隔離安全技術，並使用相同的生理信號和硬體資源來實現多個安全目標。我們還展示如何定制現有的SoC以利用更低的資源（主要是功耗），而不會對系統性能造成任何影響。

　　雖然我們提出的物聯網平台與最先進的解決方案相比具有多項優勢，但未來仍有改進的機會：

1. 包括低功率無線收發器模塊以傳輸生物醫學信號。
2. 使用ECG生成的密鑰加密和驗證通信。當前系統啟用此支持，但僅使用密鑰來解鎖鎖定的處理器。
3. 添加針對其他形式的硬體攻擊的保護，例如對加密算法的旁道攻擊。
4. 增強防止插入不同類別的硬體特洛伊木馬的保護，特別是那些易於插入和難以檢測的硬體特洛伊木馬，例如定時炸彈。
5. 將多個生物醫學信號與ECG集成，例如血糖，腦電圖和肌電圖。
6. 採用改進的濾波技術去除可能與ECG信號耦合的任何類型的噪聲，並進一步提高預測精度。
7. **結論**

　　我們提供了一個超低功耗，安全，完全集成的物聯網平台，用於使用ECG信號預測心室心律失常。所提出的架構是使用65nm LPe技術的ASIC設計流程實現的。與類似的最先進處理器相比，提議的VA處理器的功耗降低了62.2％，面積減少了16.0％。通過直接處理輸入的ECG信號來實現這種減少，因此，將用於ECG信號處理的所需RAM的大小從8KB減小到4KB。此外，對ECG信號的操作直接使得所提出的VA處理器能夠以與250Hz的採樣頻率相同的頻率操作，進一步降低了動態功耗。所提出的處理器重新使用在分類期間使用的ECG特徵來生成用於保護所提出的IoT平台免受基於遙測和基於硬體的攻擊的密鑰。整個安全基礎設施的功率和麵積開銷分別為0.7％和9.5％，對設計速度沒有影響。雖然本文提出了一個特定生物醫學SoC的案例研究，但確定安全目標並將其映射到防禦層的方法是通用的。通過一些定制，所提出的方法可以很容易地用於其他資源受限的，安全關鍵的生物醫學平台以及其他類型的物聯網設備。對設計速度沒有影響。雖然本文提出了一個特定生物醫學SoC的案例研究，但確定安全目標並將其映射到防禦層的方法是通用的。通過一些定制，所提出的方法可以很容易地用於其他資源受限的，安全關鍵的生物醫學平台以及其他類型的物聯網設備。對設計速度沒有影響。雖然本文提出了一個特定生物醫學SoC的案例研究，但確定安全目標並將其映射到防禦層的方法是通用的。通過一些定制，所提出的方法可以很容易地用於其他資源受限的，安全關鍵的生物醫學平台以及其他類型的物聯網設備。

1. **研讀心得**

經過了上學期參考文獻的訓練以及這學習論文寫作的翻譯修改練習，讓我不只在醫學工程方面的心率量測相關方法上有更多的著墨與了解，對於格式編排也能更為孰悉。在將來撰寫專業論文時奠定下基石。於此也告訴自己要多多閱讀相關的論文提升專業英文的閱讀，未來撰寫論文時也有更多的素材能使用。

　　從前是在使用者固定不動的狀態下量測心率，而現在提升至動態量測心率。在移動的情況下仍要有一定的準確度是不容易的事情。如何去除雜訊保留需要的訊號是當前重要的議題。硬體方面已有許多穿戴式的裝置應用於運動健身、健康追蹤但要達到可以提供給醫生當作遠距醫療的資料，必須要達到醫生認可的準確度才行。普遍的穿戴裝置並不具有這樣的能力，如能達成量測到達醫生希望的準確度對於遠距醫療有相當大的貢獻。在高齡化的社會趨勢下迫切的需要這樣的技術被研發出來。

　　在這篇論文中不僅提供了線上的原始碼給需要的人進行研究參考，還與多種方法進行效能評估比較。並列出了為何這篇論文中的方法優於其他演算法的原因。有許多論文提出了理論但在真實應用時並不適合使用。這篇文章的作者貢獻了他的研究在Github平台上並提到了分享知識的重要。感謝那些在Github上公開的原始碼的人，讓我在進行研究時能站在巨人的肩膀上看得更遠，省下許多時間去實現更多的想法。

**參考文獻**

1. J. Allen, “Photoplethysmography and Its Application in Clinical Physiological Measurement,” *Phys. Meas.*, vol. 28, pp. 1-39, 2007.
2. M. Hassanalieragh *et al*., “Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges,” *Proc. IEEE Int. Conf. Services Comput.,* pp. 285-292, Sept. 2015.
3. D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, “Security and Privacy for Implantable Medical Devices,” *IEEE Pervasive Comput.,* vol. 7, no. 1, pp. 30-39, Jan. 2008.
4. J. Wei, “How Wearables Intersect with the Cloud and the Internet of Things: Considerations for the Developers of Wearables,” *IEEE Consum. Electron. Mag.,* vol. 3, no. 3, pp. 53-56, Mar. 2014.
5. J. Radcliffe, “Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System,” in *Proc. Black Hat Conf. Presentation Slides*, 2011.
6. C.-I. Ieong *et al*., “A 0.83-µW QRS Detection Processor Using Quadratic Spline Wavelet Transform for Wireless ECG Acquisition in 0.35-µm CMOS,” *IEEE Trans. Biomed. Circuits Syst.,* vol. 6, no. 6, pp. 586-595, Jun. 2012.
7. R. Goyal, N. Dragoni, and A. Spognardi, “Mind the Tracker You Wear: A Security Analysis of Wearable Health Trackers,” in *Proc. ACM Symp. Appl. Comput.,* pp. 131-136, 2016.
8. C. Li, A. Raghunathan, and N. K. Jha, “Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System,” *Proc. IEEE Int. Conf. e-Health Netw. Appl. Services*, pp. 150-156, Apr. 2011.
9. M. Rostami, A. Juels, and F. Koushanfar, “Heart-to-Heart (H2H): Authentication for Implanted Medical Devices,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur*., pp. 1099-1112, Sept. 2013.
10. S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, “They can hear your Heartbeats: Non-Invasive Security for Implantable Medical Devices,” *SIGCOMM Comput. Commun. Rev*., vol. 41, no. 4, pp. 2-13, Aug. 2011.
11. N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, “ Cardiac Implantable Medical Devices Forensics: Postmortem Analysis of Lethal Attacks Scenarios,” *Digit. Investigat*., vol. 21, pp. 11-33, Jun. 2017.  
    ＊備註：此處原文未寫出刊號、頁數、年月份，只有標註出處期刊，在此補上。
12. N. Karimian, Z. Guo, M. Tehranipoor, and D. Forte, “Highly Reliable Key Generation from Electrocardiogram (ECG),” *IEEE Trans. Biomed. Eng*., vol. 64, no. 6, pp. 1400-1411, Jun. 2017.  
    ＊備註：此處原文未寫出刊號、頁數、年月份，只有標註出處期刊，在此補上。
13. G. Zheng *et al*., “Multiple ECG Fiducial Points based Random Binary Sequence Generation for Securing Wireless Body Area Networks,” *IEEE J. Biomed. Health Informat*., vol. 21, no.3, pp. 655-663, May 2017.  
    ＊備註：此處原文未寫出刊號、頁數、年月份，只有標註出處期刊，在此補上。
14. M. Rostami, F. Koushanfar, and R. Karri, “A Primer on Hardware Security: Models Methods and Metrics,” *Proc. IEEE*, vol. 102, no. 8, pp. 1283-1295, Aug. 2014.
15. J. Rajendran, O. Sinanoglu, and R. Karri, “Regaining Trust in VLSI Design: Design-For-Trust Techniques,” *Proc. IEEE*, vol. 102, no. 8, pp. 1266-1282, Aug. 2014.
16. S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, “Hardware Trojan Attacks: Threat Analysis and Countermeasures,” *Proc. IEEE*, vol. 102, no. 8, pp. 1229-1247, Aug. 2014.
17. T. Almuzaini, I. Choonara, and H. Sammons, “Substandard and Counterfeit Medicines: A Systematic Review of the Literature,” *BMJ Open*, vol. 3, no. 8, pp. 2923, 2013.
18. M. R. Shindell, T. Kramer, and S. H. Salot, “The ‘Ticking Time Bomb’ of Counterfeit Electronic Parts,” *IndustryWeek*, Jul. 2013.
19. U. Guin, D. DiMase, and M. Tehranipoor, “Counterfeit Integrated Circuits: Detection Avoidance and the Challenges Ahead,” *J. Electron. Test*., vol. 30, no. 1, pp. 9-23, 2014.
20. J. A. Roy, F. Koushanfar, and I. L. Markov, “Ending Piracy of Integrated Circuits,” *Computer*, vol. 43, no. 10, pp. 30-38, 2010.
21. J. Rajendran *et al*., “Fault Analysis-Based Logic Encryption,” *IEEE Trans. Comput*., vol. 64, no. 2, pp. 410-424, Feb. 2015.
22. M. Yasin, J. Rajendran, O. Sinanoglu, and R. Karri, “On Improving the Security of Logic Locking,” *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst*., vol. 35, no. 9, pp. 1411-1424, Sept. 2016.
23. L.T, “SypherMedia Library,” *Circuit Camouflage Technology*, Nov. 2016.
24. R. W. Jarvis and M. G. McIntyre, “Split Manufacturing Method for Advanced Semiconductor circuits,” U.S. Pat, 7 195 931, Mar. 27, 2007.
25. N. Bayasi, T. Tekeste, H. Saleh, B. Mohammad, A. Khandoker, and M. Ismail, “Low-Power ECG-Based Processor for Predicting Ventricular Arrhythmia,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*., vol. 24, no. 5, pp. 1962-1974, May 2016.
26. J. W. Schleifer and K. Srivathsan, “Ventricular Arrhythmias: State of the Art,” *Cardiol. Clin*., vol. 31, no. 4, pp. 595-605, 2013.
27. B. Mohammad, M. Al Hawari, M. Wahbah, and M. I. Elnaggar, “Autonomous Multi-Source Energy Harvesting System”, U.S. Pat, 14 601 816, Jul. 2016.
28. H. Kim, R. F. Yazicioglu, T. Torfs, P. Merken, H.-J. Yoo, and C. Van Hoof, “A Low Power ECG Signal Processor for Ambulatory Arrhythmia Monitoring System,” *Proc. IEEE Symp. VLSI Circuits*, pp. 19-20, Sept. 2010.
29. H. Kim, R. F. Yazicioglu, P. Merken, C. Van Hoof, and H.-J. Yoo, “ECG Signal Compression and Classification Algorithm with Quad Level Vector for ECG Holter System,” *IEEE Trans. Inf. Technol. Biomed*., vol. 14, no. 1, pp. 93-100, Jan. 2010.
30. S.-Y. Lee, J.-H. Hong, K.-H. Lin, C.-H. Hsieh, M.-C. Liang, and S.-Y. C. Chien, “Low-Power Wireless ECG Acquisition and Classification System for Body Sensor Networks,” *IEEE J. Biomed. Health Informat*., vol. 19, no. 1, pp. 236-246, Jan. 2015.
31. B. Colombier and L. Bossuet, “Survey of Hardware Protection of Design Data for Integrated Circuits and Intellectual Properties,” *IET Comput. Digit. Techn*., vol. 8, no. 6, pp. 274-287, Nov. 2014.
32. S. Dupuis, P. Ba, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, “A Novel Hardware Logic Encryption Technique for Thwarting Illegal Overproduction and Hardware Trojans,” *Proc. IEEE Int. On-Line Test. Symp*., pp. 49-54, Sept. 2014.
33. P. Subramanyan, S. Ray, and S. Malik, “Evaluating the Security of Logic Encryption Algorithms,” *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust*, pp. 137-143, Apr. 2015.
34. M. Yasin, B. Mazumdar, J. J. V. Rajendran, and O. Sinanoglu, “SARLock: SAT Attack Resistant Logic Locking,” *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust*, pp. 236-241, Apr. 2016.
35. R. M. Nor *et al*., “Electrocardiogram Identification: Use a Simple set of Features in QRS Complex to Identify Individuals,” in *Proc. Recent Advances in Information and Communication Technology*., Switzerland:Springer, pp. 139-148, 2016.
36. D. K. Altop, A. Levi, and V. Tuzcu, “Deriving Cryptographic Keys from Physiological Signals,” *Pervasive Mobile Comput*., vol. 39, pp. 65-79, Aug. 2017.  
    ＊備註：此處原文未寫出刊號、頁數、年月份，只有標註出處期刊，在此補上。
37. D. He, S. Chan, and S. Tang, “A Novel and Lightweight System to Secure Wireless Medical Sensor Networks,” *IEEE J. Biomed. Health Inform*., vol. 18, no. 1, pp. 316-326, Jan. 2014.
38. J. Pan and W. J. Tompkins, “A Real-Time QRS Detection Algorithm,” *IEEE Trans. Biomed. Eng.*, vol. 32, no. 3, pp. 230-236, Mar. 1985.
39. H. K. Lee and D. S. Ha, “HOPE: An Efficient Parallel Fault Simulator for Synchronous Sequential Circuits,” *Proc. IEEE/ACM Design Autom. Conf*., pp. 336-340, Apr. 1992.
40. A. L. Goldberger *et al*., “PhysioBank PhysioToolkit and PhysioNet: Components of a New Research Resource for Complex Physiologic signals,” *Circulation*, vol. 101, no. 23, pp. 215-220, 2000.
41. A. H .A., “ECRI(2008),” *American Heart Association ECG Database DVD*, Dec. 2008
42. Y.-P. Chen *et al*., “An Injectable 64 nW ECG Mixed-Signal SoC in 65 nm for Arrhythmia Monitoring,” *IEEE J. Solid-State Circuits*, vol. 50, no. 1, pp. 375-390, Jan. 2015.