這篇論文提出了一種解決方案，讓低成本的消費者物聯網（IoT）設備能夠實現端到端的安全性，而無需額外的硬件支持。消費者物聯網設備的製造商往往為了提供更多功能、使用友好性、上市時間或成本而犧牲安全性，以保持競爭優勢。然而，這是不明智的，正如最近對消費者物聯網設備的駭客攻擊所證明的那樣。低成本的嵌入式設備往往難以創建適當的熵以進行密鑰生成；另一方面，智能手機既豐富又具有多個源頭的熵，可以用於生成強大的密鑰。所提出的架構利用了這些特性，將密鑰生成和傳輸外包給用戶的智能手機，從而消除了受限制的IoT設備執行公鑰基礎設施並生成對稱密鑰的需要。作者在一款價格為1美元的通用微控制器上實現了這一設計，然後進行了性能分析。該設計允許設備的所有通信都進行加密，同時設置簡單、成本低廉且響應迅速，而無需額外的製造成本。該架構提供了一種通用的解決方案，可以在任何微控制器上實現。由於這種架構不需要任何額外的硬件，因此可以通過固件更新後向已部署的設備進行後續應用。

I. 簡介

最近，消費者行為的發展推動了家居自動化設備市場的增長。這些設備承諾使我們的生活更加便利和自動化。例如，可以使用語音助手、智能手機或自動觸發器（例如接近家庭時）開啟和關閉燈光。雖然自動化系統已經存在多年，但隨著技術的改進以及設備的成本和安裝難度的降低，消費者物聯網（IoT）設備在家庭設置中的需求迅速增加[1]。然而，這種便利和低成本也伴隨著風險。最近有許多家庭互聯網連接設備被入侵的案例[2]–[5]。然而，由於家庭消費市場對價格敏感，這對於使設備安全化提出了挑戰。實施安全功能可能會導致製造商的成本增加[6]。本文將重點放在家庭低成本Wi-Fi IoT設備上，並探討引入強大安全性的方法。

II. 背景

A. 市場限制

隨著物聯網（IoT）設備市場的持續增長，最近一份英國國會科學與技術辦公室的報告[7]將經濟驅動因素列為導致消費者設備網絡安全性差的主要原因之一。歐盟網絡安全局、學術界和行業都表示，製造商將成本、用戶體驗和上市時間置於安全性之上[8]–[12]。此外，一項2017年的調查發現，42%的製造商的消費者不願意為安全性支付費用，而下一大部分消費者（28%）只願意支付1-10%的額外費用[13]。這意味著安全性必須在不增加硬件成本的情況下提供。

B. 安全性

高級加密標準（AES）使用一個共享密鑰來快速高效地加密和解密數據，即使在成本較低的設備上也可以實現[14]，[15]。這可以通過純軟件或硬件加速版本來實現。這種類型的加密的主要不足之處在於需要在兩個端設備上使用相同的密鑰，這導致了在設備之間安全地共享密鑰的挑戰[16]。克服這個問題的傳統方法是採用混合加密。公開金鑰加密用於建立一個安全通道，該通道用於傳輸共享的對稱密鑰[17]，[18]。這種方法在高性能計算設備（如智能手機）上表現良好，但不太適用於成本較低的嵌入式硬件。

C. 安全需求

消費者物聯網（IoT）設備可以分為兩類：可以本地支持安全性的設備和需要額外硬件才能安全通信的設備。前者由性能相對較高的設備組成，通常具有ARM芯片和/或運行完整操作系統的能力。其中一種設備是Google Chromecast，它具有AES硬件加速器和隨機數生成器[19]，因此能夠實現公開金鑰基礎設施並生成適當的隨機對稱密鑰來加密未來的通信。

在第二類中，有許多受限制的設備只設計用於單一有限的目的，它們使用性能較低的計算硬件來實現其主要功能。這些性能較低的芯片通常不具備硬件AES加速器或硬件隨機數生成器。此外，由於這些設備遵循可預測的事件序列，它們難以生成足夠的熵來創建安全密鑰。一個受限制的設備的例子是Belkin Wemo Switch，該設備為客戶提供了遠程打開和關閉任何插入主電源插座的設備的能力。用戶還可以使用他們的智能手機檢查他們是否已經關閉了特定的電器，當他們到達家中時觸發燈光開啟，或者以程序方式安排設備開啟或關閉，從而為消費者節省金錢和時間。然而，產品發布不久後，人們發現了設備架構中的各種漏洞，導致Belkin建議客戶不再使用該產品。這些漏洞是可能的，因為Belkin採用了基於密碼的加密來生成AES密鑰，其中密鑰的參數是可預測的。

通信通道的安全性取決於用於加密該通道的密鑰的不可預測性；因此，需要適當的隨機熵來確保生成強大的密鑰。如果攻擊者可以預測憑證，即使是最複雜的安全方案也會因為猜測密鑰而被破壞。對於傳統通信，這不是一個問題，因為現代計算機和智能手機已經從各種不同的來源獲取熵，可以將其結合起來。然而，在低成本的物聯網設備中生成適當健壯的密鑰更具挑戰性。這些設備通常運行一個有限的指令集，並且幾乎沒有用戶交互作用。作為回應，研究界已經探討了各種潛在的解決方案，以使受限制的嵌入式設備能夠生成適當的熵。

LoRaWAN聯盟試圖通過重複使用現有硬件來解決這個問題，即單一用途的設備不夠複雜，無法生成足夠的熵。注意到這些設備必須具有天線來發送和接收消息，因此將天線用作傳感器，記錄接收信號強度。這被認為是足夠隨機的，但研究人員發現，通過干擾或其他方式影響信號強度，它可能變得更加可預測。這表明，儘管現有的傳感器可能是可用的，並且可以提供半隨機的數據，但如果傳感器受到影響，這將導致熵源質量不佳。

學術研究人員確實發現，當使用額外的硬件時，嵌入式設備可以產生足夠的熵。Voris等人調查了使用各種單個傳感器，包括加速度計、磁力計、接近傳感器、光度計、溫度計和麥克風，並發現每個傳感器都會產生一些熵。然而，所有這些傳感器都受到外部干擾的影響，除了加速度計。

研究人員接著發現，任何試圖減少加速度計生成的熵的企圖都將導致熵的增加。這表明使用加速度計將是在高度受限的設備中提供熵的解決方案。同樣，具有AES硬件加速器和硬件隨機數生成器的加密身份驗證協處理器能夠產生足夠的熵。最後，研究人員發現某些特定的微控制器實現可以利用其硬件生成熵。然而，重要的是要注意所有這些解決方案僅適用於特定情況，而不是通用解決方案。由於那些未具備這些特性的設備，其原材料成本將會增加。

立法正在跟上這個問題。最近加州參議院法案第327號[31]規定，製造商在加州銷售設備前必須做出合理的網絡安全嘗試。雖然這只直接影響加州，但製造商可能會普遍應用這些變化，以避免維護兩個不同版本的設備。另一方面，最近英國消費者物聯網安全守則[32]概述了一些物聯網安全的改進措施，但目前僅是自願性的。同樣，歐洲電信標準化協會（ETSI）還概述了製造商可以自選遵循的13項做法[33]。法規2019/881還建立了歐洲聯盟網絡安全機構，其任務是為歐盟在網絡安全事務上創建認證框架和治理結構[34]。然而，在撰寫本文時，尚未制定具體規則。在美國，2019年的物聯網網絡安全改進法案[35]旨在利用美國聯邦政府的購買力說服物聯網製造商提高其設備的安全性。然而，這項法案目前還在立法程序中，並且也僅僅是自願性的。

III. 架構

我們的解決方案使用智能手機來安全地生成加密材料，然後將其傳遞給消費者物聯網設備以及物聯網設備的伺服器。智能手機在英國的普及率達到87%[36]，而在智能家居目標人群中，擁有至少一部智能手機的比例高達95%[37]。智能手機擁有強大的處理器、多種傳感器、豐富的用戶互動功能，並且能運行多個進程，因此非常能夠生成足夠的隨機數據來提供適當的隨機密鑰[26]。將密鑰傳輸到物聯網設備也利用了現有技術，因為物聯網設備本身已經具備了連接互聯網的能力。

Google對其流行的基於Wi-Fi的Chromecast設備採用了表面上相似的設置程序，在設置過程中使用智能手機將物聯網設備連接到家庭Wi-Fi網絡。這種方法也已經為家用電器申請了專利[38]。然而，Chromecast能夠發起TLS連接，因為它配備了Marvell DE3005-A1片上系統[19]，其中包含硬體隨機數生成器和AES硬體加速器。低成本、低功耗的設備則不具備任何這些額外的硬體。

安全初始化協議的操作如下：

1. 該設備在出廠時被預配置了一個（理想情況下是唯一的）WiFi憑證，並將該憑證提供給用戶隨包裝一起。
2. 在首次激活時，該設備使用此憑證設置一個私人網絡，用戶使用其智能手機連接到此網絡。
3. 智能手機播種隨機數據並生成一個AES密鑰。
4. 智能手機將此密鑰與物聯網設備共享，並共享物聯網將用於連接互聯網的網絡憑證。
5. 智能手機和物聯網設備從私人網絡斷開連接並重新連接到互聯網。
6. 智能手機和物聯網設備使用智能手機生成並共享的密鑰通過本地網絡建立一個對稱加密的安全連接。
7. 智能手機安全地將物聯網設備的密鑰共享給遠程服務器。

在啟動時，該設備將使用默認的SSID和設備專屬的密碼廣播其Wi-Fi接入點，這與英國《消費者物聯網安全守則》[32]一致。這些密碼將在工廠中預配置到設備中，並可選擇以QR碼的形式提供在產品包裝內。這種方法的一個額外優勢是可以自動化使用63字符長的Wi-Fi密碼，同時消除用戶輸入時可能出現的人為錯誤。

在運送途中，有可能出現封包被攔截的情況，即惡意行為者打開封包並記錄提供的QR碼，以在設備設置過程中攔截AES密鑰的傳輸，從而危害設備安全。然而，可以採取以下幾個額外步驟來減少這些風險。

1. 降低設備的Wi-Fi發射功率：將物聯網設備的Wi-Fi發射功率調至最低，例如ESP8266的最低功率為0.25 dBm，這樣當嘗試在距離超過20厘米的地方檢測信號時，信號會消失在噪聲底層。Android手機的Wi-Fi自適應功率控制也會相應地減少手機的發射功率。
2. 配置Wi-Fi模組以支持單一連接：因此，暫時的Wi-Fi網絡在任一時間只能由一個惡意攻擊者或合法用戶連接。
3. 將QR碼封裝在防篡改信封中。

此外，2.4 GHz Wi-Fi頻段高度擁擠【39】, 因此惡意攻擊者在房屋外等待時，很難檢測到正確的信號。此外，臨時Wi-Fi網絡只會配置為大約一分鐘的廣播時間，這比典型的按鈕壓Wi-Fi保護設置（WPS）時間更短。

伴隨的應用程序可以從應用市場下載，例如Google Play商店，該應用程序會生成AES密鑰並自動連接到私有網絡。啟動此過程時，用戶會掃描QR碼，應用程序會提取憑證並將智能手機的Wi-Fi從家庭網絡切換到IoT設備生成的網絡。然後，智能手機會生成AES密鑰並將其傳輸到IoT設備。隨後，應用程序會提示用戶輸入任何特定信息，例如個性化的設備標識符和IoT設備加入網絡的家庭Wi-Fi憑證。

當密鑰共享完成後，兩個設備都會重新加入家庭網絡。一旦IoT設備和智能手機能夠在網絡上相互識別，連接過程就會被認為是成功的。最後，智能手機將引導用戶完成可選步驟，將設備連接到外部服務器，以便在家外控制。智能手機將通過建立SSL/TLS連接來安全地傳輸AES密鑰。此時，手機、開關和服務器應該能夠相互聯繫並加密/解密所有消息。如圖1所示，所提出的架構基於本地交互，然後將密鑰發送到遠程位置，而不是嘗試從遠程位置提供唯一密鑰。這將提供以下優點：

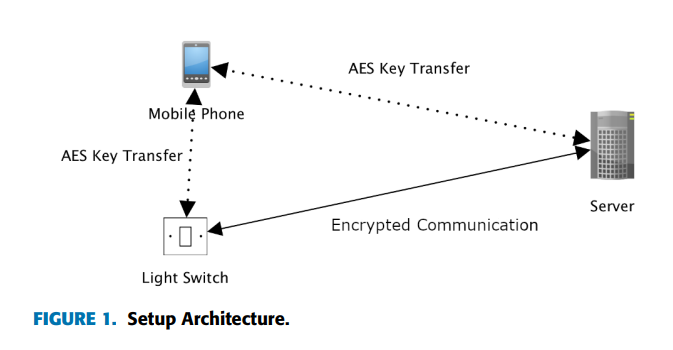


圖 1. 設定架構。

* 如果用戶不希望從家外控制其設備，則不需要外部通信。
* 如果製造商的伺服器宕機或停用，產品仍可繼續運行，而在類似情況下其他設備可能會失去功能。在所有這些情況下，設備都可以默認為本地運行並且仍然在本地可用。
* 產品製造商不需要生成和管理密鑰的分發。
* 通過短期私人網絡傳輸密鑰，家庭網絡上的受損設備無法竊聽密鑰。在設備加入家庭網絡後傳輸密鑰會有被攔截的風險。
* 用戶在物聯網設備中輸入高熵密鑰的過程得到了極大簡化。

B. 內部用戶通信

移動應用通過監視網絡實現無需集中式中心的內部通信。

在檢測到新開關時，移動應用會向用戶發出提示，提示他們開始安裝過程。如果任何開關丟失了其先前分配的地址，定期搜索還會找到並記錄IP地址的任何變化。這種方法的缺點是，網絡中的任何惡意設備都可以通過其指紋檢測到物聯網設備的存在。然而，考慮到設備可以通過其他幾種技術進行檢測，這被認為對於所有通信都將被加密來說影響很小。

C. 外部用戶通信

當物聯網設備處於不同的網絡上時，通信是通過 API 端點管理的。授權觸發器，例如用戶的手機、語音助手（如 Google Home、Alexa、Siri）或自動化應用程序（如 IFTTT、tasker、zapier），都可以連接到製造商的服務器，向相關的端點發送 HTTP 請求，並更新設備的狀態。然後，物聯網設備將定期輪詢中央服務器並相應地更新。

IV. 實施

這個提出的架構已經被實現，創建了一個物聯網智能燈開關，使用了一個 MSP430G2553 微控制器和一個 ESP8266 Wi-Fi 芯片。智能開關可以通過燈開關上的物理按鈕和 Android 應用程序來控制。該應用程序在本地網絡上本地運行，也可以通過一個集中式服務器遠程運行。與集中式服務器的連接還允許開關成為更大系統的一部分。例如，還設置了一個與 Google Home 助手配合使用的 IFTTT 配方，以便通過語音控制燈光。

A. 設備設置

如第三部分所述，智能開關的設置是通過將開關接線並加入其創建的私人Wi-Fi網絡來完成的，以傳輸在Android手機上生成的AES密鑰。應用程序還可用於個性化詳細信息，例如為燈光命名，以便用戶在應用程序中知道他們正在修改的燈光，例如主臥室。一旦完成這些步驟，用戶可以決定是否授權外部連接。如果他們同意，應用程序將與中央服務器建立安全連接，將燈光的詳細信息和相關的AES密鑰傳輸到用戶的遠程帳戶。

B. 內部通信

鑑於該系統設計為無需外部服務器或本地中心運行，Android手機使用mDNS檢測將自己宣傳為智能開關的設備，並將消息使用相關的AES密鑰加密。接收到的開關通過檢查HMAC確認消息的真實性，然後解碼並對消息進行操作。

C. 外部通信

每當有亮度變化，無論是通過應用程序還是燈開關的實際變化，設備都會向服務器發送HTTP POST請求，更新遠程保存的燈狀態。一旦用戶打開移動應用程序，就會發出HTTP請求以調整顯示以反映確切的亮度。在狀態更改請求時，將向服務器發出請求以更新狀態。智能開關設備將每30秒輪詢一次服務器，如果檢測到爭端，則物理按鈕將覆蓋服務器狀態。

D. 加密

可預測的消息，如開和關，可能透過分析模式來推斷家中是否有人居住。此外，如果這些消息每次保持不變，則可能會記錄消息以進行重放攻擊。因此，決定在服務器、Android應用程序和智能開關上實現AES計數模式，以掩蓋消息，並通過實現類似於LoRaWAN規範中規定的計數器來防止重放攻擊。為了防止位翻轉攻擊，每個設備還計算了消息身份驗證碼（MAC），並將其包含在發送的消息中。接收設備在解密有效載荷之前檢查MAC。

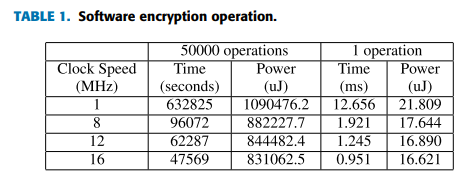


表 1. 軟體加密操作

V. 結果

儘管智能開關實現是作為一個概念證明，但所提出的架構適用於任何低成本的物聯網設備。考慮到這一點，對系統的時間和能量需求進行了測量，用於在MSP430G2553上運行AES128軟件實現。在測試過程中，發現測量設備的準確度不足以測量單個加密/解密操作。因此，決定執行該過程50,000次，並推斷出每個加密和解密操作的單個操作所需的需求。還決定變化MSP430G2553芯片的時鐘速率，以比較消耗的時間和能量。加密的數據顯示在表1中，完成單個AES加密操作需要15,725個周期。

軟件解密的實現也進行了分析。雖然發現需要23,470個周期，比加密算法增加了。測試表明，AES128加密和解密都適用於大於25毫秒的響應時間。這顯然低於250毫秒的人類響應時間平均值。時序和能量消耗詳細列於表2中。作者指出，雖然在較低的時鐘頻率下功耗較低，但1 MHz時鐘操作的增加時間要求導致使用最高的總消耗。因此，根據應用程序，可能更有利於以最高功耗 - 16MHz - 運行，然後啟用其中一種內置的低功耗模式。另一方面，如果系統設計為持續運行且未啟用任何低功耗模式，則以1MHz運行將節省功耗。表3詳細說明了不同時鐘速度下固定間隔10秒的功耗，以及低功耗模式3的功耗。

如上所述，保護低成本物聯網設備的三個問題是：密鑰生成、建立公鑰加密和保持響應性。將生成工作卸載到智能手機解決了第一個問題。使用同一智能手機來傳輸密鑰解決了第二個問題。最後，通過證明在MSP430G2553上加密和解密可以在合理的時間內實現，所提出的架構解決了所有概述的問題，使得一個1美元的微控制器可以使用AES128。

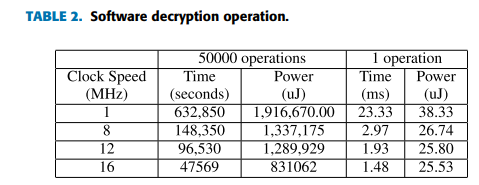


表 2. 軟體解密操作

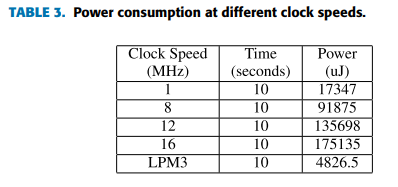


表 3. 不同時脈速度下的功耗。

提出的架構對於單個用戶或多個共享相同密鑰的用戶運作良好。然而，如果每個用戶需要專用密鑰，例如為燈提供分區控制。每個用戶都必須為他們被允許控制的每盞燈重複設置過程，這是一項耗時的任務。這個問題的簡單解決方案是讓每個新用戶通過mDNS檢測到他們可以看到的所有開關，並為每個開關生成一個新的密鑰。然而，由於這些密鑰將在家庭Wi-Fi網絡上傳輸，如果這個網絡被破壞，那麼每個密鑰也將被破壞。一個更複雜的解決方案涉及創建一個主用戶。主用戶將創建主AES密鑰，最初設置所有設備。一旦控制權要轉交給新的個人，將生成新的子密鑰並使用主密鑰對所需的每個開關進行加密後傳送。然後，主用戶將分別使用藍牙或NFC將每個子密鑰傳送到用戶的手機上。然而，在這些受限制的設備中存儲進一步的密鑰將需要更多資源，並且對用戶來說會更加複雜，因此，如何在特定情況下進行進一步操作將取決於供應商的決定。

所提出的架構是針對Wi-Fi設備進行了定制，因為大多數家用物聯網設備市場使用Wi-Fi。儘管如此，類似的想法也可以應用於可穿戴設備，這些設備主要使用藍牙與智能手機連接。此外，通過修改設計以通過本地中介（例如中心）中繼數據，還可以使用智能手機上通常不常見的其他通信接口。例如，飛利浦Hue使用Wi-Fi與中心通信，然後使用Zigbee與燈泡通信。中心作為手機生成的密鑰的中繼，將允許每個飛利浦Hue燈泡對其流量進行端到端加密。可以進一步進行工作以實現此修改。

這一創建的架構使得低成本的物聯網設備能夠擁有足夠隨機的密鑰，而無需額外的專用硬件。通過將密鑰生成和傳輸外包給用戶的智能手機，不需要額外的組件來生成熵。此外，通過外包密鑰傳輸，不需要強大的處理器來進行安全的公鑰加密，因為這些處理器大部分時間都是閒置的。本文還詳細介紹了這種系統的功耗和時間要求。我們展示了使用我們的方案，由於加密開銷，響應速度的延遲將小於25毫秒。該架構還提供了一種用戶友好的方式來安全地設置設備，並結合最近關於物聯網設備安全的立法，證明了這種架構將是有益的。具體而言，該架構允許低成本的物聯網設備進行端到端的加密，保護免受“中間人”攻擊、UPnP漏洞和同一網絡上的惡意設備的威脅。將此架構應用於貝爾金Wemo開關將防止這些設備被利用，如上文所述。此外，由於該架構不需要額外的硬件，因此可以通過固件更新部署到現有設備上。最後，由於該架構與平台無關，因此可以部署到任何後端Web服務器上，並且對於其他形式的沒有Wi-Fi連接的物聯網設備進行輕微修改。