國立清華大學 電機工程學系
實作專題研究成果報告

A study of Laser Fault Injection Detector in 7nm FinFET Platform

基於 7nm 鰭式電晶體平台的激光故障注入檢測器研究

專題領域：電子領域

組　別： B466

指導教授：林崇榮教授

組員姓名：陳鈺蓁、吳若歆

研究期間：113 年 2 月 22 日至 113 年 11 月 25 日止，共 9 個月

I. 摘要

在現代數位安全的發展中，Physical Unclonable Function (PUF)成為一種重要的安全機制，然而，儘管 PUF 表面上具備極高的安全性，其實也深受 Laser Fault Injection (LFI)的威脅。LFI 被公認為是一種針對高安全性設備最為有效且破壞性極大的攻擊手段，攻擊者透過精確的雷射注入干擾電路，進而可能影響 PUF 的功能或洩露其內部資訊，威脅設備的安全性。

為了有效應對 LFI 所帶來的威脅，本研究以簡單有效的 CMOS inverter 做為 detector 檢測 LFI 攻擊，並與 sense amplifier 結合，確保檢測的正確性。並且我們也將 detector 和 D-latch 結合，以確保輸出的穩定性。藉此產生能夠即時並有效檢測 LFI 的 detector 系統。

本研究自尺寸設計、雷射 pulse width 考量及 Vbias 調整等三個面向著手設計 detector，完成 detector 設計後，將其輸出端與 sense amplifier 的 enable 連接，當 LFI 發生，SA 的 output 做出響應，藉此偵測雷射攻擊。接著，再將 detector 輸出端與 D-latch input 連接，當 LFI 發生，D-latch 直接反應 detector output 的變化，藉此穩定並快速的偵測雷射攻擊。

II. 報告內容

1 背景與動機

隨著物聯網、嵌入式系統以及加密技術的快速發展，硬體安全的重要性日益凸顯。作為硬體安全的一項關鍵技術，Physical Unclonable Function (PUF) 憑藉其無法複製的特性，被廣泛應用於身份驗證和密鑰生成。然而，PUF 的安全性並非無懈可擊。

fault injection attack(FIA)利用 fault injection(FI)分析加密功能的方法，藉此比對有無故障的密文，在眾多攻擊手段中，Laser Fault Injection (LFI) 成為對 PUF 安全性威脅最大的技術之一。LFI 通過精確的雷射干擾，可擾亂 PUF 的輸出，從而削弱 PUF 在加密和防偽中的應用價值。

由於 LFI 的高效性與廣泛性，如何快速檢測攻擊成為一項急需解決的技術挑戰。現有的防護方法多數專注於加強 PUF 本身的設計，但對攻擊的即時檢測與反應機制研究仍然不足。

在硬體安全領域中，檢測往往比防護更具實用性與成本效益，特別是在面對未知或不可完全避免的攻擊時。快速而準確的檢測機制，能在攻擊發生時提供即時的反應，避免因攻擊延遲檢測而造成的更大損害。若 PUF 能搭配一個能有效監測電路是否是到 LFI 攻擊的檢測器，就能使 PUF 在硬體安全的應用上有近一步的發展。

2 研究目的

在現代數位安全的發展中，Physical Unclonable Function (PUF)利用製程上的物理變異來實現其獨特的隨機性，由於製程差異受到多種因素的影響，例如製造環境和溫度，這些差異具有高度的不可預測性和不可控性，因此能夠提供安全且無法仿造的硬體識別。然而，看似如此安全的 PUF，卻也深受 Laser Fault Injection(LFI)威脅，LFI 被認為是破解高安全性設備時最有效的攻擊方法，為了應對 LFI 帶來的威脅，設計一套有效的 LFI detector 顯得格外重要，透過即時監測電路及硬體是否受到攻擊，並在攻擊發生的第一時間做出反應，減少對電路的破壞，進而提升 PUF 在對抗 LFI 時的安全性。

3 研究方法

3-1. Paper researching

透過大量文獻閱讀，累積相關背景知識，並從中擷取有用的資訊，加以整合利用，並發想研究內容。根據[1]，FIA 包含 Voltage and timing glitches, Laser fault injection, Electromagnetic fault injection, Electrostatic discharge impact, …以下分別簡略介紹。

3-1-1. Voltage and timing glitches

在電源引腳施加高電壓或低電壓尖峰，或在時脈訊號中插入窄脈衝的矩形波，

可能導致電路發生錯誤。例如，可能會讓正反器或閂鎖誤保持錯誤的邏輯值。此方法相對簡單且成本低廉。

3-1-2. Laser fault injection(LFI)

使用雷射從 IC 晶片的背面穿過矽基板照射微處理器。光子能量轉換會激發電子 - 電洞對，這些電子和電洞會移動到電源電壓和接地，產生電流並在照射位置附近引起電壓波動 (VSUB)。這可能會導致記憶體匯流排上的位元改變以及指令管道中的指令跳過。LFI 是針對精細線路 IC 晶片技術最精密的攻擊手段。

3-1-3. Electromagnetic fault injection(EMFI)

讓 IC 晶片暴露於高功率射頻 (RF) 電磁波，引發意外的位元翻轉或操作中斷，以干擾區域取決於天線的大小，射頻信號的頻率和功率會被廣泛掃描和重複以尋找故障輸出。

3-1-4. Electrostatic discharge impact(ESDI)

使用 ESD 槍在倒裝晶片組裝中 IC 晶片的背面產生電壓突波。ESD 保護結構（反向偏置二極體對）可能會導致 ESDI 產生的電壓毛刺遠離 ESD 保護二極體的位置，導致錯誤輸出。

綜合以上的分析，我們認為 LFI 是最具威脅性的攻擊方法，除了具有高定位性，也具有很好的故障位元誘導能力和良好的再現性，是非常強大的攻擊方式。因此，本實驗以檢測 LFI 為目標，期望可以達到即時檢測，進而有效防範。

3-2. Detector 設計

根據[2]，4tOS 在監測 LFI 具有靈敏度、尺寸、可靠性等多項優勢，因此，我們以此為基礎發想，決定使用如 Fig.1 的 detector 架構，當雷射攻擊發生時，光電流會導致 Vin 電壓下降，進而改變 NMOS(MN1)和 PMOS(MP1)導通狀態，使輸出發生改變，當攻擊結束，PMOS(MP2)會將 Vin 充到 VDD，使電路能對後續攻擊做出反應。並且以 MP1 尺寸調整、Laser Pulse Width 測試及 Vbias 調整三個面向，在25℃ TT corner下，找出最適合的 detector。

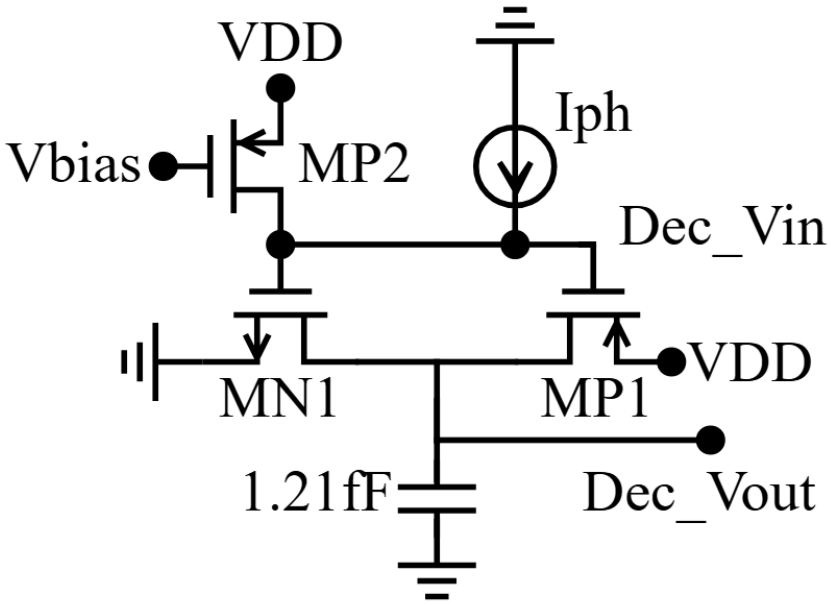

Fig.1 Detector 架構

3-2-1. PMOS(MP1)尺寸調整

我們對不同 PMOS Fin 數進行 sweep，分析其對檢測器反應時間的影響。結果顯示，隨著 Fin 數增加，反應時間也相應增加，因此我們選擇了適合的 Fin 數來優化檢測速度。

當 PMOS fin 數量增加，反應速度主要受 gate capacitance 影響，造成放電時間上升，反應時間上升，因此我們最後選擇 fin=3 來進行後續的設計。

3-2-2. Pulse Width 測試

我們對雷射 Pulse Width 進行了掃描，發現當脈衝寬度減少到 14ps 以下時，檢測器無法達到 0.9 倍的 VDD，導致反應失效。這一結果有助於設定檢測器的最佳脈衝寬度範圍，以保持檢測精度。

3-2-3. Vbias 調整

我們進行了不同 Vbias 設置的模擬，發現當設置的模擬，發現當 Vbias 過低時，時，PMOS 和和 NMOS 都處於次臨界區導致反應時間延長，這表明我們需要精確控制確控制 Vbias 以保證穩定的反應時間。

為確保設計的實用性，本研究也在不同溫度及 corner 下測試 detector 的穩定性。我們給定 0.1mA 的電流模擬 LSF，設定 VDD=0.8V。

測試方式：量測 Iph 打入至 Vout 升起至 0.9 倍 VDD 的 response time

量測區間：−40℃~120℃、分別測試 TT FF SS FS SF 五個 corners

測試結果如下表所示，在不同的測試區間，response time 都相去不遠，代表 detector 能夠在不同的環境下維持其工作效率。

Table.1 response time(ps) under different conditions

	-40C	25C	120C
TT	17.4	20.3	17.8
FF	26.35	24.5	22.78
SS	13.73	14.21	15.15
FS	15.08	15.45	16.25
SF	22.15	21.25	20.5

3-3. sense amplifier

3-3-1. sense amplifier(SA)運作行為

如 Fig.2 右側所示，SA 主要由 NMOS（MN3 與 MN4）、PMOS（MP3 與 MP4），以及由 SAEN 控制的 NMOS（MN5）組成。一開始 bit_line 和 bit_line_b 會先被預充電到 VDD。當記憶體陣列中的某個存儲單元被選中時，該單元會通過 bit_line 產生一個微小的電壓差。

當 SAEN 上升時，M5 導通，感測放大器啟動。此時，由於 bit_line 和 bit_line_b 之間的電壓差，M1 與 M2 的導通程度不同，造成流經兩條分支的電流產生不對稱。M3 與 M4 的正反饋作用進一步放大了這個不對稱信號，使得微小電壓差迅速被放大成的高電位與低電位，分別為 SA 的輸出 out 和 out_b。這種電路設計具備高靈敏度，能快速放大微弱的差分信號，提升了整體的效率。

3-3-2. Detector 與 sense amplifier 整合

在此研究中，我們將 detector 和 SA 進行整合，主要目的是防止攻擊者透過雷射攻擊干擾記憶體資料，整體架構如 Fig.2 所示。Detector 主要負責檢測雷射攻擊是否發生，當雷射發生時 Detector 的輸出電壓會上升，而我們的目的是雷射發生時停止電路運作，為此我們在中間加入一些邏輯控制電路去實現此功能，我們在 Detector 和邏輯控制電路之間加入一個 inverter，主要目的是將 Dec_Vout 的極性翻轉，以生成符合 SA 所需求的 SAEN 訊號。具體來說，當雷射攻擊發生，Dec_Vout 會升高，而 SA 需要 LOW 的 SAEN 來停止運作。

當 ENABLE=HIGH 時，SA 的狀態由 detector 的輸出電壓狀態決定:一，雷射未發生時，Dec_Vout 為 LOW，經過 inverter 後 SAEN 為 HIGH，此時 SA 正常運作；二，當雷射發生時， Dec_Vout 為 HIGH，經過 inverter 後 SAEN 為 LOW，此時 SA 停止運作，防止攻擊者獲取有效的差分訊號放大結果。另一方面，當 ENABLE=LOW 時，無論雷射是否發生，SA 皆會停止運作。

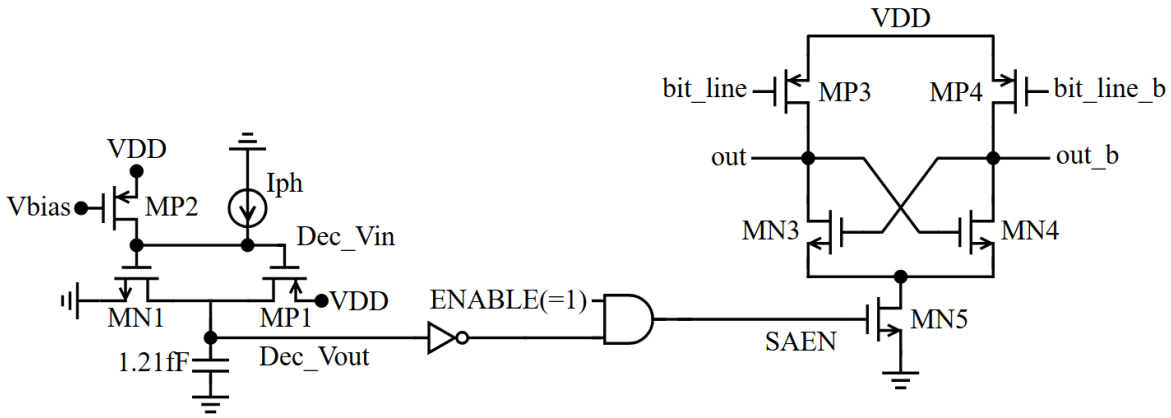

Fig.2 Detector with sense amplifier 架構

為確保 detector 運作的準確性，本研究將 detector 以 Fig.2 的方式與 SA 進行整合，detector output 經過 inverter 與 ENABLE 訊號 AND 後，接至 SA 的 SAEN 訊號，透過觀察 SA 的 output 變化，判斷是否發生雷射攻擊。

3-4. D-latch

3-4-1. D-latch 運作行為

當 Enable =1：
D 輸入的資料會即時傳遞到輸出 Q（即 Q = D）。
此時進入透明模式（Transparent Mode），輸入直接控制輸出。

當 Enable =0：
鎖存器鎖住當前的輸入狀態，Q 的輸出保持不變（即使 D 改變）。
此時為保持模式（Latch Mode）。

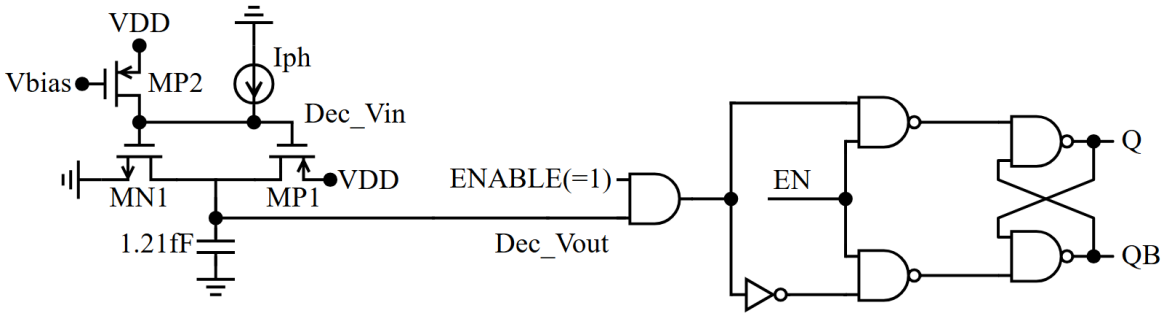

Fig.3 Detector with D-latch 架構

3-4-2. Detector 與 D-latch 整合

運用 D-latch 的特色，可以確保 detector 運作的穩定性，本研究將 detector 以 Fig.3 的方式與 D-latch 進行整合。在 detector 偵測到 LFI 時，發送 alarm 訊號與 EN 做 AND，此輸出再傳至 D-latch，成為 D-latch 的輸入 D。

4 研究結果

4-1. Detector 與 sense amplifier 整合成果

Fig.4 為模擬 laser pulse = 2ns，Detector 與 sense amplifier 整合後的波形圖，當發生 LFI 時(藍色區塊)，如 Fig.4 所示，當 Pulse Width 為 2ns 時，可以看出沒發生雷射攻擊(Region I)，整個 SA 是正常運作的，在 7ns~9ns(bit_line 為 HIGH、bit_line_b 為 LOW)和 9ns~11ns(bit_line 為 LOW、bit_line_b 為 HIGH) ，out 和 out_b 正確的反應差分訊號的放大結果，當 bit_line > bit_line_b 時，out 被拉至低電位；bit_line < bit_line_b 時，則為 out_b 被拉至低電位 。當雷射發生的時候 (Region II)，由於檢測器觸發使 SA 關閉，可以看出 out 和 out_b 皆被 pull up 到高電平，不再反應差分訊號，這種行為說明，我們阻止了 SA 對 bit_line 之間的微小電壓差進行放大，從而有效防止攻擊者獲取正確的數據。

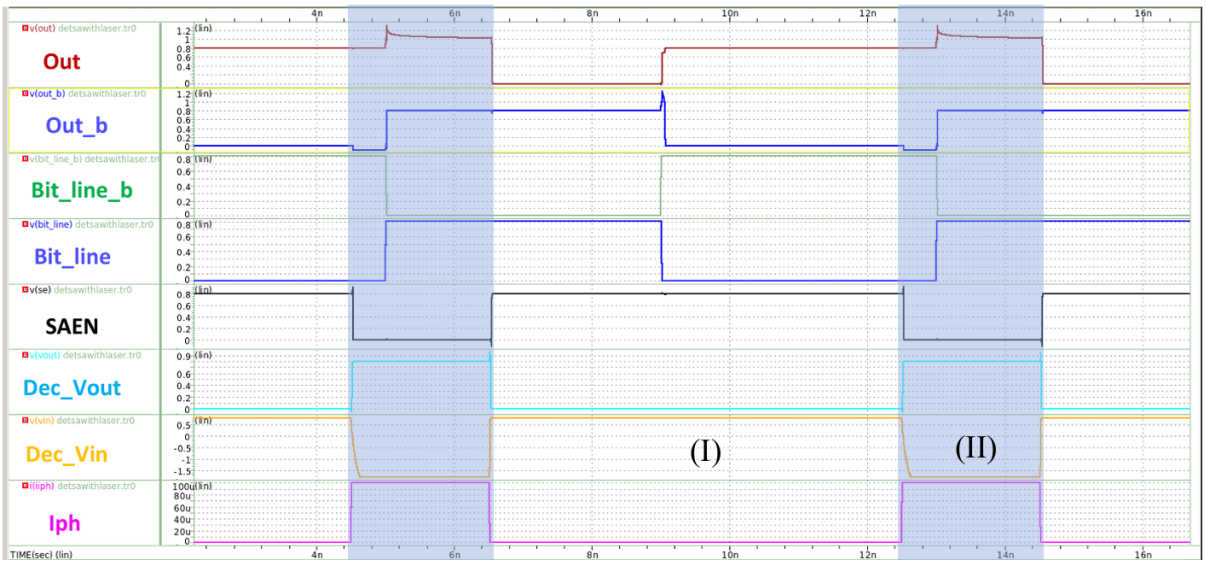

Fig.4 wave view when pulse width = 2ns

4-2. Detector 與 D-latch 整合成果

分別以 laser pulse = 2ns 與 laser pulse = 0.2ns 進行模擬，Fig.5 為 laser pulse = 2ns 時，EN 的訊號週期設為 1ns，藍色區塊為 Iph 產生電流模擬 LSF，電路遭到攻擊，此時 vin 被 pull down，dec_vout 抬升，將此訊號傳送至 D-latch 的 input，因 EN=1，值直接傳送之 Q 輸出，LSF 至 Q 產生反應的 delay 為 36.2ps。藉由觀察 Q 升起的波型，來監測電路受到攻擊的情況。

當 laser pulse = 0.2ns 時，EN 的訊號週期設為 0.2ns，藍色區塊模擬電路遭到 LSF 攻擊，同樣能藉由觀察 Q 的變化得知電路受到攻擊的情況，LSF 至 Q 產生反應的 delay 為 36.2ps。

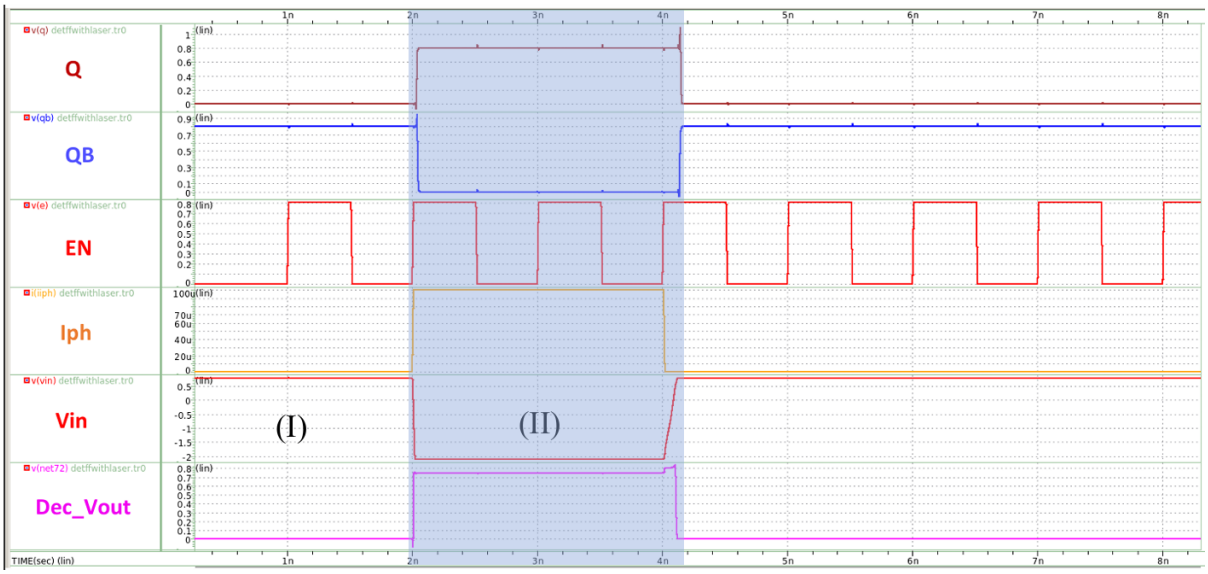

Fig.5 wave view in pulse width = 2ns

5 結論

本研究針對 Laser Fault Injection(LFI)設計一套穩定的 LFI 檢測架構，整合了 LFI Detector、Sense Amplifier 以及 D-latch。檢測器基於 CMOS 結構，具備高靈敏度與穩定性，能迅速響應雷射攻擊的瞬態變化，即使在不同製程條件和極端溫度下（-40℃至 120℃）仍表現出穩定性能。在檢測器與 SA 的結合中，當檢測到雷射攻擊時，能迅速關閉 SA，阻止攻擊者利用差分訊號竊取數據；而檢測器與 D-latch 的結合則能有效記錄攻擊事件，並提供穩定的輸出。通過對檢測器關鍵參數（如 MP1 Fin 數與 Vbias）進行優化。模擬結果表明，當 Laser Pulse Width 相較於基準值（2ns）縮短達 90%（僅為 0.2ns）時，仍能成功檢測並記錄攻擊，展現出極高的靈敏度和安全性。整體設計結構簡單，易於實現，適合應用於高安全性硬體防禦系統中，為提升硬體安全性提供了一種可靠且高效的解決方案。

III. 心得

在這歷經兩個學期的專題中，首先由林崇榮教授帶領我們進入這個未知的領域，初步了解 fault injection 的概念，在第一個學期，我們透過閱讀許多相關論文，整理並融會貫通其中的知識點後，第二個學期開始，我們便以 4tOS 的架構為出發點，首先檢測 detector 的適用性，接著再結合 SA 與 D-latch，形成一個穩定的檢測器架構，能確實達到快速偵測攻擊的效果。

在研究的過程中，通常會先確定這周的進度內容，兩人分派各半的工作，如果我們有遇到問題，會先向彼此討論，若是仍無法解決，便會向林唯華學長請教，在完成一些進度後，我們也會彼此交流自己做的內容與當中遇到的困難，並且向學長報告最近的進展。

在此感謝林唯華學長的帶領與指導，在研究過程給予我們許多建議，也感謝林崇榮教授願意擔任我們的指導教授，並帶領我們在這個領域有更多的認知。

IV. 參考文獻

[1] M. Nagata, "Exploring Fault Injection Attack Resilience of Secure IC Chips : Invited Paper," 2022 IEEE International Reliability Physics Symposium (IRPS), Dallas, TX, USA, 2022, pp. 11C.1-1-11C.1-6, doi: 10.1109/IRPS48227.2022.9764485.

[2] D. Zooker, Y. Weizman, A. Fish and O. Keren, "Silicon Proven 1.29 μm × 1.8 μm 65nm Sub-Vt Optical Sensor for Hardware Security Applications," in IEEE Access, vol. 11, pp. 136269-136278, 2023, doi: 10.1109/ACCESS.2023.3338001.