D18-034

對於互聯網裝置使用真隨機變數方法與偽隨機控制器的DC-DC開關轉換器的安全機制

An Enhanced Security Buck DC-DC Converter with True Random Number (TRN) Based Pseudo Hysteresis Controller for Internet-of-Everything (IoE) Devices

隊伍名稱　玖壹貳 Nine One Two
隊　　長　歐陽佑政 / 交通大學電機工程學系
隊　　員　朱立程 / 交通大學電控工程研究所
　　邱俊愷 / 交通大學電機工程學系
　　林彥安 / 交通大學電機工程學系

指導教授

陳科宏
交通大學電機工程學系

臺灣大學電機工程學系學士、碩士、博士，現職交通大學電機工程學系教授兼系主任。2004年成立混合訊號及電源管理晶片積體電路實驗室，已發表逾240篇論文於國際知名期刊及會議，並於2016年出版電源管理晶片設計專書Power Management Techniques for Integrated Circuit Design。陳教授現任IEEE Transactions on Power Electronics副主編、IEEE Transactions on Circuits and Systems I: Regular Papers副主編、Analog Integrated Circuits and Signal Processing編輯委員，同時為ISCAS、ESSCIRC等大會議程委員，並擔任2018年10月International Workshop on PwrSoC之共同大會主席，主辦此世界首屈一指的電源轉換器相關應用整合會議。

研究領域

電源管理積體電路設計、低功率電路設計、混合訊號電路設計、無線充電晶片設計、綠能電子。

作品摘要

傳統基於線性反饋移位暫存器的迴路隨機化技術雖具有防衛功率旁路攻擊之能力，但在功率注入攻擊下，由於線性反饋移位暫存器之可預測性和重複性，導致其所產生之隨機數受到限制，進而造成迴路隨機化技術被破解並失去防衛功率旁路攻擊之能力。此外，功率注入攻擊不僅縮小了基於線性反饋移位暫存器之隨機切換頻率範圍，還會將傳統基於三角波調變技術之調變頻率降低至切換頻率之約1/N倍，故使得電磁干擾雜訊頻譜無法符合EN 55032 Class B之規範。而在其他使用反制方式以提高硬體安全性之技術中，則會大幅地增加功耗或增加硬體成本。

為了同時防衛功率旁路攻擊、功率注入攻擊並降低電磁干擾而不降低性能，本研究提出了增強安全性的隨機數產生器和基於真隨機數的偽遲滯控制器。前者能夠在功率旁路攻擊與功率注入攻擊下仍正常地產生獨立於輸入電壓之隨機數。後者則能將此隨機數轉換成遲滯窗以實現真隨機調變之切換頻率，從而確保適當展頻範圍與低電磁干擾。

本研究所提出之建立在真偽隨機變數上的增強型安全機制直流降壓轉換器同時提高了對PSCA和PIA的安全性。採用AOFC技術的SA-TRNG能夠確保即使在1V的PIA干擾之下，隨機變數的分布與平均值能夠達到安全性的效果。測得最高的峰值電壓干擾從89.72dBμV到54.32dBμV，但是因為增強型機制隨機變數的產生，滿足EN55032B的要求，在PSCA和PIA的干擾下能夠正確的生成與輸入電源無關的隨機變數。最後，測量的結果顯示瞬態響應下，恢復時間為7.3μs。在切換頻率為1MHz的狀態下，在負載從0.2A瞬間拙至0.8A的情況下，輸出電壓瞬間下降，峰對峰值效率為92.4%。

在未來科技的演進之下，IoE設備應用通常指的是更長時間的睡眠模式或待機模式。待機模式下的功耗會直接的影響到IoE設備的使用壽命。具體而言，控制器的靜態電流會支配空載或者是超輕載下的功耗，因此，我們追求的是在不降低對方攻擊性能和安全性的情況下實現最低的靜態電流。

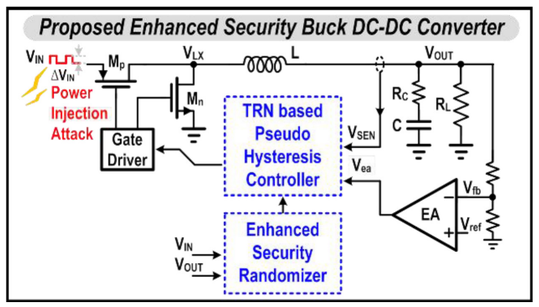

圖1. 本作品之電路架構示意圖

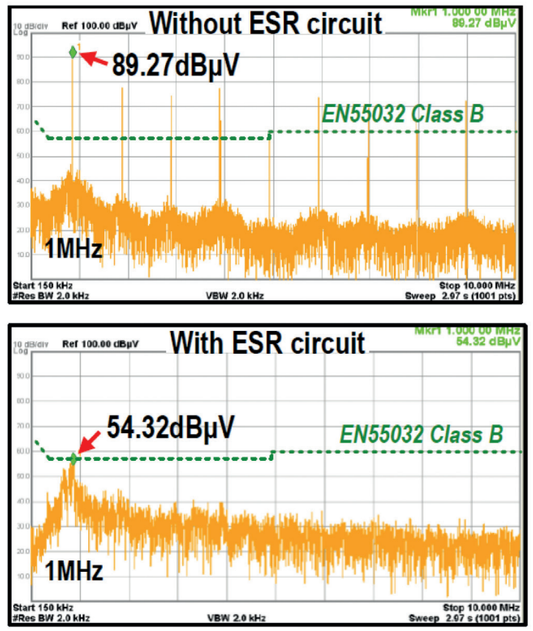

圖2. 針對抵抗電磁干擾採用增強型安全機制之功效比較圖

Abstract

As far as Internet-of-Everything (IoE) devices are concerned, strong hardware security and low electromagnetic interference (EMI) are design requirements for power management to guarantee personal data protection. Conventional linear feedback shift register (LFSR) based loop randomization technique has the ability to avoid the power side channel attacks (PSCA), but the power injection attack (PIA) results in limited random number (RN) due to the predictability and reproducibility of the LFSR, and thus cause the loop randomization cracked and vulnerable to the PSCA. Besides, the PIA not only narrows the LFSR based random switching frequency but also reduces the triangular modulation frequency to around 1/N times of the switching frequency. Consequently, the EMI noise floor fails to meet the specification of EN 55032 Class B. Other techniques offer counter-measures to improve resistance against malicious attacks but result in either greatly increased power consumption or large hardware overhead.

In this work, the true random number (TRN) based pseudo hysteresis controller (PHC) and the enhanced security randomizer (ESR) are proposed to avoid both PSCA and PIA simultaneously and reduce EMI without degrading performance. The ESR is capable of generating input-supply-independent RN correctly under PSCA and PIA. The TRN based PHC converts the RN to the hysteresis window that constitutes a true random modulated switching frequency, thereby ensuring suitable spread spectrum and low EMI.

In this work, the proposed buck converter with TRN based PHC and ESR enhances security against the PSCA and PIA simultaneously. The SA-TRNG with AOFC technique guarantees the distribution and average of the random number even under 1V PIA interference. Measured peak electromagnetic interference noise decreases from 89.72dBμV to 54.32dBμV since the ESR meets the EN 55032 Class B requirement as the enhanced security randomizer generates input-supply-independent RN correctly under PSCA and PIA. Finally, measured results show the transient performance of 7.3μs recovery time and 53mV drop of output voltage in case of 0.2A-to-0.8A load step at the fSW around 1MHz with the peak efficiency of 92.4%.

In these days, the applications of IoE devices usually refer a long sleep time and standby mode. The power consumption at standby mode directly affects the usage time of the IoE devices. Specifically, the quiescent current of the controller dominates power consumption at no-load or ultra-light load condition. As a result, achieving low quiescent current of the controller without degrading the performance and the security against malicious attacks is an interesting topic.

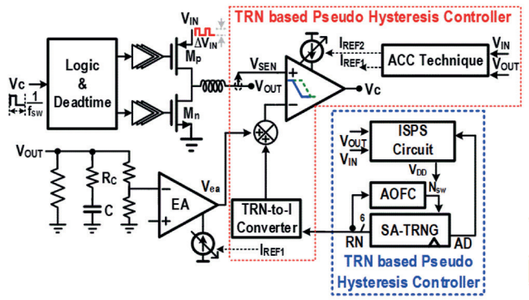

Fig.3 TRN based pseudo hystersis controller