An Encrypted On-Chip Power Supply With Random Parallel Power Injection and Charge Recycling Against Power/EM Side-Channel Attacks

Kang Wei, *Member, IEEE*, Jin Woong Kwak, *Student Member, IEEE*, and D. Brian Ma, *Senior Member, IEEE*

***Abstract*— As hardware security becomes a crucial challenge for modern electronic devices to protect information privacy, this article presents an encrypted on-chip power supply to combat power and electromagnetic (EM) side-channel attacks (SCAs) for crypto cores. By splitting power and security into separate paths, random parallel power injection and charge recycling are realized to encrypt supply power activities for high SCA immunity while largely minimizing power and performance overheads. Despite of crypto core power variations, the proposed power supply can maintain uncorrelated input profile by adaptively modulating parallel noisy power injection. Moreover, its EM leakage is highly attenuated by spreading the spectrum energy to a wide frequency range and increasing noise floor. To achieve such, a recycled masking power stage with an encryption interface is designed to randomly inject power noise and recycle system charge with random ON-time modulation while still retaining nominal power delivery. A silicon IC prototype of this design is fabricated using a 65 nm CMOS process with an active die area of 0.19 mm^2. Measured input power profiles are fully encrypted to improve power SCA immunity. Operating at a nominal switching frequency of 10 MHz, random parallel power encryption reduces peak EM interference noise from 64.57 dBμV to 43.12 dBμV to meet EN55032 Class B standards and verify EM spectrum profile encryption. In response to a step-up load change from zero to full load current of 200 mA, the power supply achieves 1% settling time of 0.78 μs, with measured voltage droop of 54 mV with no other performance overhead. It achieves a peak efficiency of 90.5%, only suffering the maximum power overhead of 4.9%.**

***Index Terms*—Charge recycling, encrypted on-chip power supply, hardware security, power/EM side-channel attack, random ON-time (ROT) modulation, random parallel power injection.**

Manuscript received 16 May 2022; revised 27 July 2022; accepted 8 September 2022. Date of publication 13 September 2022; date of current version 10 October 2022. This work was supported in part by the Semiconductor Research Corporation under the research task of SRC GRC 2810.055. Recommended for publication by Associate Editor C. N. M. Ho. *(Corresponding author: D. Brian Ma.)*

Kang Wei was with the Integrated Power System Laboratory, the Department of Electrical and Computer Engineering, the University of Texas at Dallas, Richardson, TX 75080 USA. He is now with the Texas Instruments, Dallas, TX 75243 USA (e-mail: kang.wei@ti.com).

Jin Woong Kwak and D. Brian Ma are with the Integrated Power System Laboratory, the Department of Electrical and Computer Engineering, the University of Texas at Dallas, Richardson, TX 75080 USA (e-mail: jinwoong.kwak@utdallas.edu; d.ma@utdallas.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TPEL.2022.3206182.

Digital Object Identifier 10.1109/TPEL.2022.3206182

I. Introduction

TODAY'S information explosion drives a significant number of electronic devices to connect through wireless networks for end-to-end communications. In order to protect information privacy, hardware security has emerged as a crucial challenge for modern electronics. Although cryptographic cores are widely developed to perform data encryption, these devices can be still easily cracked with side-channel attacks (SCAs) [1], [2], [3], [4], [5], [6]. As encryption usually causes unique switching patterns, vital side-channel information such as power and electromagnetic (EM) profiles can be stolen and statistically analyzed to retrieve plaintext, making cryptographic algorithms no longer effective. Among different types of SCAs, the most powerful one is power side-channel attack (PSCA) as power usage of digital ICs is highly related to data inputs. Therefore, simple and differential power analysis were first introduced to directly investigate supply power profiles and predict secrete encryption keys. Afterward, correlation power analysis was developed to assess the correlation between measured power profiles and predicted power model for correct key retrieve. This reduces the minimum number of power measurements to key disclosure to only a few thousands with low cost and easy deployment [2].

Numerous PSCA countermeasures have been reported in the past [3], [4], [5], [6], [7], [8], [9]. First, crypto engine algorithms and implementations are upgraded to make secret key more difficult to predict [3], [4]. However, this increases circuit complexity and performance overhead significantly. In addition, it is incompatible with various encryption schemes. The second countermeasure concept is to make power usage of digital logics independent of data variations. Power-balanced circuits such as dual-rail precharge logic and wave dynamic differential logic (WDDL) are reported for such [5], [6]. However, these solutions induce power penalties and large area overheads due to the complexified digital circuitry. Last, recent research efforts mainly encrypt supply power profiles to enhance security and reduce overhead of crypto cores. This can be realized by combining power encryption with integrated power supplies, which are commonly used in modern SoCs. Therefore, linear regulators, switched-capacitor circuits, and switch mode power converters are specifically designed to decorrelate power profiles from the switching activities of encryption cores [7], [8], [9]. However, severe tradeoffs originally observed in secure crypto cores will

be automatically shifted to the implementation of integrated power supply. This makes it challenging to realize accurate voltage regulation and energy loss and cost minimization while securing side-channel leakage.

In addition to the foregoing countermeasures, randomization is highly favorable to mask critical side-channel information and reinforce security. Thus, random switching is widely applied to secure power supplies by randomizing feedback regulation loop [9], [10]. However, the range of such randomization is limited narrowly. Otherwise, dramatic loop randomization compromises system stability and could trigger system malfunction. Besides, the circuit designs of such mostly rely on digital random number generators (RNGs) with linear feedback shift registers [9], [10]. However, the dependency of available random numbers on supply voltage causes a pivotal threat to cryptographic security if the attackers manipulate power input voltage physically through power injection attack (PIA) [10].

While power analysis requires direct measurements of crypto core power consumption, EM analysis enables an indirect SCA by simply interpreting EM radiation pattern that is correlated to the crypto encryption algorithms [11]. This type of noninvasive attack can be easily performed in the middle of cryptographic operation without physical interruption. Thus, in order to protect crypto cores against direct and indirect SCAs, both power and EM profiles correlated to data encryption must be kept hidden during entire run time.

Several countermeasures have been proposed to suppress the inadvertent EM side-channel leakage of crypto cores [7], [9], [12]. Similar to the countermeasures against PSCAs, random noise injection and feedback loop randomization are used to attenuate the leaked EM spectrum amplitudes, hindering the statistical analysis of EM side-channel leakage [7], [9]. However, these approaches will largely increase switching noise on crypto core supply voltage and require sophisticated compensation network to stabilize system control. Besides, a security-aware metal routing technique is presented with randomization of power regulation to encrypt EM profiles by synthesizing crypto cores at lower-level metal layers and covering critical circuitries with upper-level metal routing [12]. However, this specific security-aware metal routing technique requires multiple metal layers, which is not in favor of low-cost silicon IC processes.

As an optimized countermeasure against power and EM SCAs, an encrypted on-chip power supply is presented in this article to achieve power profile encryption with largely reduced power and performance overheads. Instead of merging security feature with power delivery in prior solutions, the proposed power supply uses a recycled masking power stage to separate security feature from main power path, enabling system balance among performance, power, and security. Besides, random parallel power injection and charge recycling are utilized to only encrypt input power $I_{\rm IN}$ profile while retaining nominal system switching action. This helps the on-chip power supply to realize easy combination of noise injection, supply masking and switching randomization to enhance power security and realize EM profile encryption with reduced electromagnetic interference (EMI) noise. With an encryption interface (EI), a recycled masking power stage is precisely regulated by random ON-time (ROT) modulation to inject noisy power and deliver system power efficiently even if power input voltage $V_{\rm IN}$ is physically varied. The remainder of this article is organized as follows. Section II reviews current SCA countermeasures and describes system architecture of the proposed encrypted on-chip power supply. Section III elaborates the system and circuit implementations. Experimental results are provided in Section IV for design validation. Finally, Section V concludes this article.

II. System Architecture and Operation

A. State of Current SCA Countermeasures

With power supplies commonly integrated on-chip, there are great potentials to embed SCA countermeasures without affecting encryption algorithms or circuits. Multiple techniques are presented to accomplish such, which can be categorized as noise injection, supply masking, and switching randomization. Fig. 1(a) shows the circuit diagram of noise injection. To create a parallel current noise $I_{\rm NOISE}$, a short circuit (SC) can be used as the pseudoload current $I_{\rm SC}$ [13], which is switched by a random clock $V_{\rm CLK}$ with a RNG. The PSCA mainly relies on the statistical correlation coefficient between the $I_{\rm IN}$ and the core power $I_{\rm CORE}$, which can be calculated as

$$\rho_{I_{\rm IN},\ I_{\rm CORE}} = C_{\rm ov}\ (I_{\rm IN},\ I_{\rm CORE}) \,/\, (\sigma_{I_{\rm IN}} \times \sigma_{I_{\rm CORE}}), \qquad (1)$$

where C_{ov} and σ represent covariance and standard deviation of the matrix, respectively. Because $I_{\rm IN}$ is equal to the sum of actual supply current I_S and $I_{\rm NOISE}$, (1) can be rewritten by combining $I_{\rm IN} = I_S + I_{\rm NOISE}$ as

$$\rho_{I_{\rm IN},\ I_{\rm CORE}} = C_{\rm ov}\ (I_S,\ I_{\rm CORE}) \,/\, \left(\sqrt{\sigma_{I_S}^2 + \sigma_{I_{\rm NOISE}}^2} \times \sigma_{I_{\rm CORE}}\right). \qquad (2)$$

Here, $I_{\rm NOISE}$ is assumed to be independent of $I_{\rm CORE}$. Compared to I_S, $I_{\rm IN}$ profiles are largely decorrelated from $I_{\rm CORE}$ by increasing $I_{\rm NOISE}$ variance and reducing the signal-to-noise ratio (SNR) of $I_{\rm IN}$. However, a large $I_{\rm NOISE}$ is normally discharged by the SC to the ground, increasing power penalty significantly. A current-domain signature attenuation is reported in [12] to mitigate this. A shunt bleed transistor and a local load capacitor are used to compensate $I_{\rm CORE}$ variations such that $I_{\rm IN}$ profile is attenuated and the injected $I_{\rm NOISE}$ can be largely reduced. However, it still induces nearly 50% power overhead and the design of power circuits and bleed transistor become more complicated if system power demand is increased by advanced encryption cores.

Alternatively, Fig. 1(b) shows the circuit diagram of supply masking. An intermediate power rail $V_{\rm INT}$ is switched ON or OFF to mask side-channel information leaked from encryption cores. The core supply voltage $V_{\rm CORE}$ is regulated to determine if $V_{\rm INT}$ is connected to $V_{\rm IN}$ for power rail charge or supplied to $V_{\rm CORE}$ for core power delivery. This is implemented in [14] by using two input decoupling capacitors to deliver $I_{\rm CORE}$ alternatively under encryption. Thus, the timing information is protected to make post processing alignment more difficult for PSCAs. Besides, it can easily manipulate $I_{\rm IN}$ profile by adjusting capacitor voltages. However, using

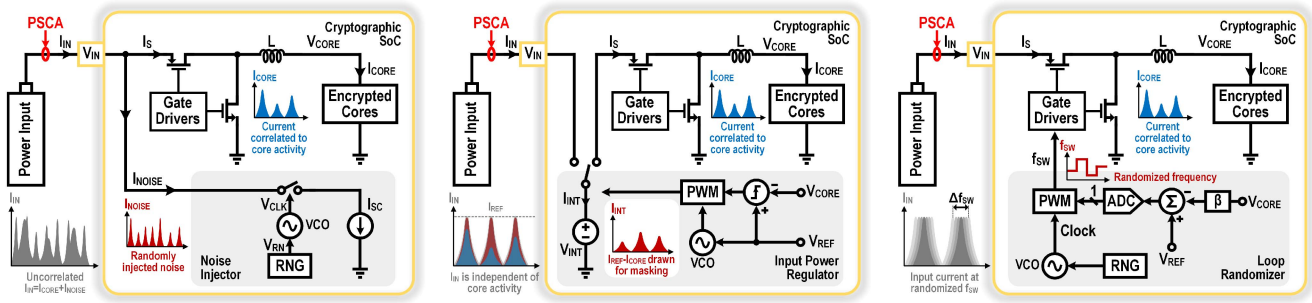


Fig. 1. Illustrations of existing SCA countermeasures: (a) noise injection approach, (b) supply masking approach, and (c) switching randomization approach.

two capacitors could cause unreliable line regulation, potential supply voltage glitch, and system failure. A switched-capacitor current equalizer is used in [15] to precisely regulate only one capacitor and achieve constant $I_{\rm IN}$ profiles. However, the capacitor has to be discharged additionally to a fixed voltage in each switching cycle, largely increasing power consumption. Large capacitance is critical to reduce supply voltage ripples, which, unfortunately, increases silicon area and fabrication cost.

Instead of exploring specialized circuit techniques, switching randomization is a more generic solution due to its compatibility to most integrated power supplies. More importantly, this approach can protect crypto devices against power and EM SCAs at the same time, making it superior to the aforementioned approaches. As shown in Fig. 1(c), a random clock is widely used to randomize system switching frequency ($f_{\rm SW}$) through feedback loop. In [9], an integrated inductive voltage regulator employs loop randomization to add pseudorandom delay in digital pulsewidth modulation (PWM) control. Moreover, a pseudo-hysteresis controller is presented in [10] to randomly modulate $f_{\rm SW}$ by adjusting hysteretic windows with true random numbers. However, Fig. 1(c) illustrates that the random sources introduce a separate control variable, which conflicts with the regulation purpose of the main feedback loop. Therefore, system stability must be carefully examined and more complex compensation networks are required to stabilize system. Furthermore, supply voltage variations can be only reduced by narrowing randomization range, resulting in the tradeoff between security and system performance.

B. Proposed Encrypted On-Chip Power Supply

The discussion above indicates that existing countermeasures face momentous challenges to balance system performance, power, security, and cost. The fundamental cause is that security features have been integrated into power circuits, without considering adverse effects between each other. Consequently, design specifications such as efficiency, voltage regulation, and SCA immunity are compromised. Hence, it motivates this work to propose an encrypted on-chip power supply, which splits power and security into two parallel connections to avoid design conflicts and thus greatly alleviate system tradeoffs. Moreover, side-channel security is improved by simultaneously realizing noise injection, supply masking, and switching randomization without performance degradation and large overheads.

The system architecture of the proposed encrypted power supply is detailed in Fig. 2(a). In addition to a classic dc–dc power stage for conventional power delivery, a recycled masking power stage is added, which utilizes charge and discharge paths of on-chip temporary power storage unit (a capacitor in the prototype of this work) as a parallel input power branch to create noisy current $I_{\rm PI}$ for power injection and thus mask $I_{\rm IN}$ profile. To reduce power overhead, system charge on the capacitor can be efficiently recycled by conveying the discharge current $I_{\rm CR}$ to supply $I_{\rm CORE}$. Random ON-time ($T_{\rm ON}$) modulation is implemented in an EI to precisely regulate capacitor voltage $V_{\rm CS}$, randomize switching activities of main power stage and retain clock synchronization between parallel connections. Meanwhile, the injected $I_{\rm PI}$ can be adaptively adjusted to attain the uncorrelated $I_{\rm IN}$ profile despite the change of $I_{\rm CORE}$. Thus, random parallel power injection and charge recycling are successfully realized with simple structure to improve power security and reduce overhead and silicon area.

Fig. 2(b) describes the operation schemes of this encrypted power supply. First, by activating the charge of a capacitor in the parallel branch while the main power I_S is delivered to $I_{\rm CORE}$, an adaptive current noise $I_{\rm PI}$ is generated to store extra charge ΔQ to the capacitor $C_{\rm CS}$. Thus, $I_{\rm IN}$ is manipulated by power injection to retain the uncorrelated profile and hide key $I_{\rm CORE}$ variations. Afterward, the stored ΔQ is recycled by $I_{\rm CORE}$ to minimize power overhead. To achieve such, the main power conversion stage is disconnected from $V_{\rm IN}$ and the capacitor $C_{\rm CS}$ is configured as an internal supply rail to transfer energy through $I_{\rm CR}$ with consistent switching as main power branch. This not only enhances energy efficiency and maintains system performance but also protects the timing of $I_{\rm CORE}$ variations from exposure. Random $T_{\rm ON}$ modulation is finally used to decide whether the power branch or the capacitor $C_{\rm CS}$ is enabled for core power delivery. Switching randomization is hence introduced to largely decorrelate $I_{\rm IN}$ profiles from $I_{\rm CORE}$. Thanks to the recycled masking power stage, the encrypted power supply secures $I_{\rm IN}$ by randomly redistributing the charge required by $I_{\rm CORE}$, facilitating random power injection and charge recycling for high security and low overhead.

On the other hand, the EMI noise spectrum in Fig. 2(c) shows that the proposed power supply can effectively attenuate the

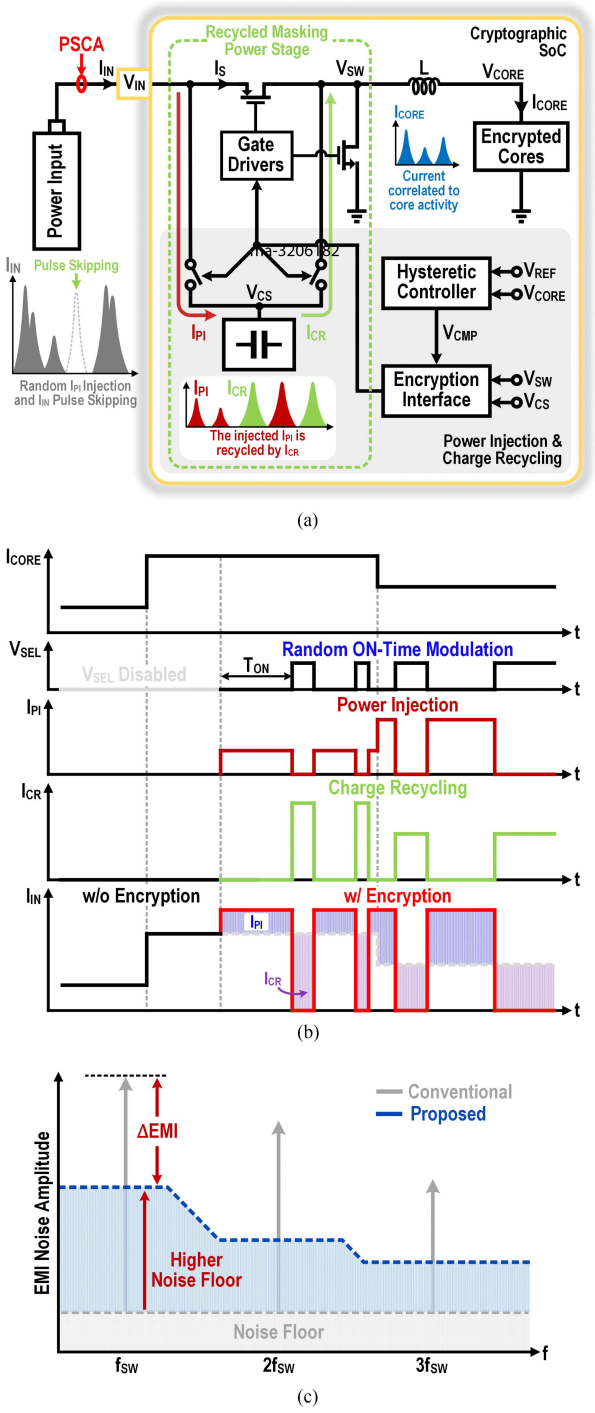


Fig. 2. (a) System architecture, (b) operation scheme, and (c) EMI noise spectrum of the proposed encrypted on-chip power supply.

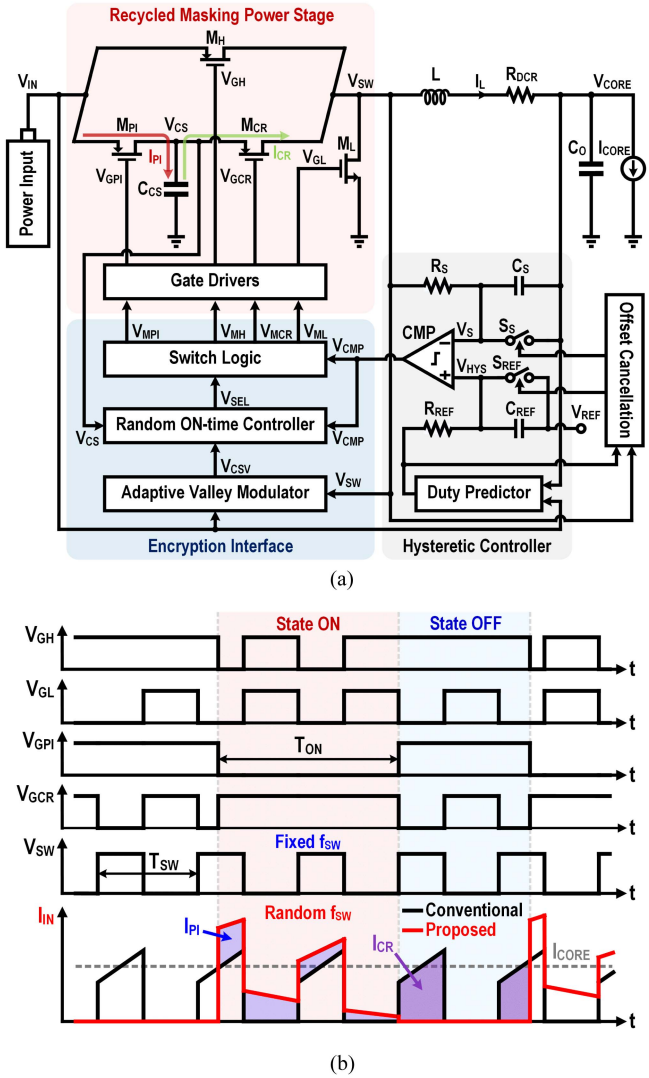


Fig. 3. (a) Circuit implementation of the encrypted on-chip power supply, and (b) timing diagram of the recycled masking power stage.

peak EMI noise at fundamental f_{SW} and increase entire noise floor. Due to random T_{ON} modulation, the input current pattern of this power supply is randomized, spreading most of EMI spectrum energy to a wide frequency range with a higher noise floor. This helps to suppress the EMI peak by ΔEMI and provide uncorrelated EM profile. That is, it becomes much more difficult to detect the peak EMI noise originally correlated to the activity of the encryption core, preventing EM SCA successfully.

In comparison with prior arts, this power supply effectively combines three major encryption techniques of noise injection, supply masking, and switching randomization to decorrelate I_{IN} and I_{CORE} significantly. By distributing I_{IN} randomly, it benefits peak EMI noise reduction and thus encrypts EM profile against SCA. As only I_{IN} is modified while retaining normal switching, control complexity is significantly reduced with nearly zero performance overhead. Moreover, it realizes charge recycling to lower power penalty for highly efficient SCA countermeasure.

III. Circuit Implementations

A. Recycled Masking Power Stage

The circuit implementation of the encrypted on-chip power supply is illustrated in Fig. 3(a). It mainly includes the parallel power stage of an EI and a recycled masking power stage, and a hysteretic controller. The hysteretic controller is used to realize precise voltage regulation with fast load transient response [16]. A duty predictor provides the expected switching

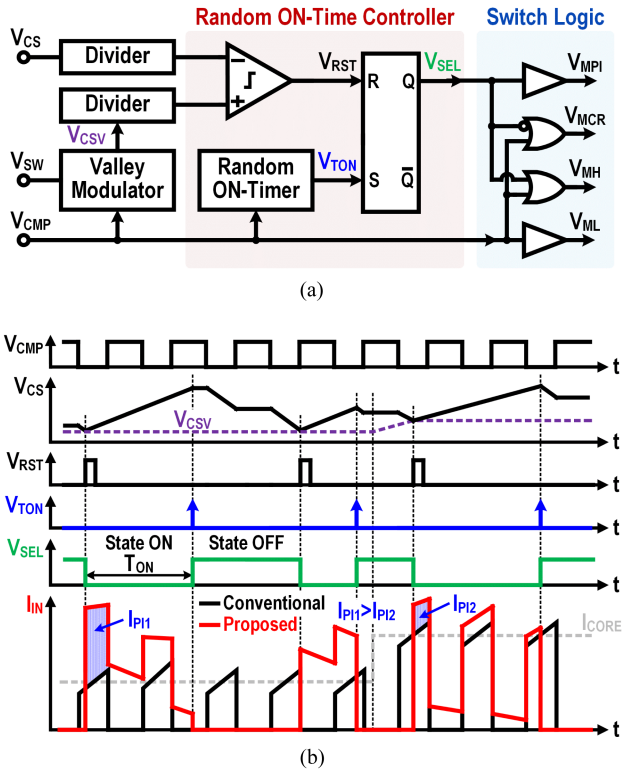


Fig. 4. (a) Circuit diagram, and (b) operation timing diagram of the EI in the proposed encrypted power supply.

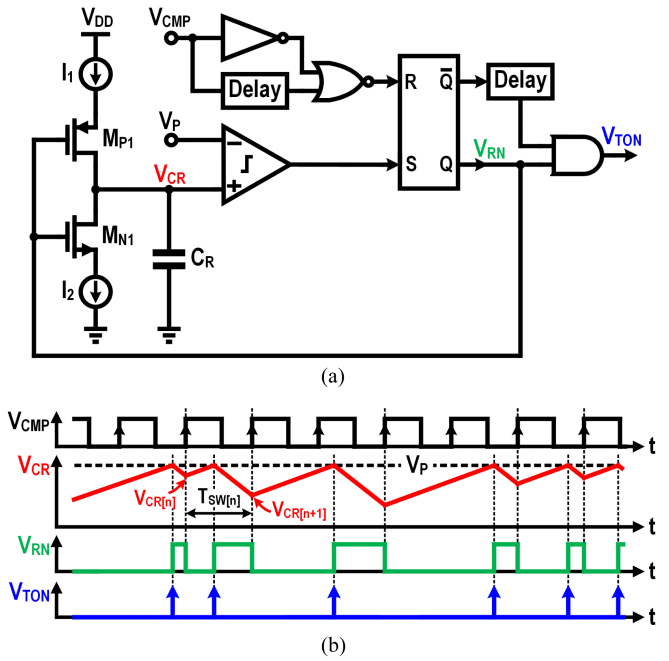


Fig. 5. (a) Circuit schematic, and (b) operation scheme of the random ON-timer.

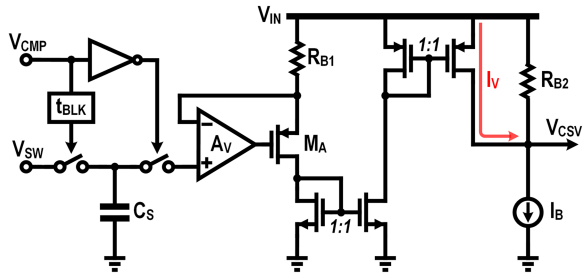


Fig. 6. Circuit implementation of the adaptive valley modulator.

voltage information and modulates the hysteretic bound $V_{\rm HYS}$ adaptively through a RC matching filter $R_{\rm REF}C_{\rm REF}$. The R_SC_S matching filter is used to sense the inductor current I_L for fast current-mode feedback control. Two reset switches S_S and $S_{\rm REF}$ eliminate $V_{\rm CORE}$ offset caused by the dc resistance (DCR) of the inductor L. The recycled masking power stage adds two switches $M_{\rm PI}$ and $M_{\rm CR}$ and one capacitor $C_{\rm CS}$ in parallel with main power switch M_H. It operates with two states ON and OFF in each switching cycle. Once the state ON is activated, $C_{\rm CS}$ is charged by $V_{\rm IN}$ while switches M_H and M_L remain nominal switching for power delivery. After this state is disabled by the EI, the state OFF is triggered to shut down input power and make $C_{\rm CS}$ serve as a supply rail. $M_{\rm CR}$ is treated as high-side switch along with M_L to operate in the consistent switching manner as the state ON. Overall, states ON and OFF enable power injection and charge recycling, respectively, for low overhead SCA countermeasure.

The timing diagram of the recycled masking power stage is shown in Fig. 3(b). In the state ON, $M_{\rm PI}$ is turned ON to connect $C_{\rm CS}$ to $V_{\rm IN}$ during the entire on-duty time $T_{\rm ON}$. Because $V_{\rm CS}$ is discharged to be lower than $V_{\rm IN}$ when the state ON is initialized, $C_{\rm CS}$ is charged by $V_{\rm IN}$ continuously with the charge current of

$$I_{\rm PI} = I_{\rm PI0} \times e^{-t/R_{\rm ds,PI}C_{\rm CS}}, \tag{3}$$

where $R_{\rm ds,PI}$ represents the on-resistance of $M_{\rm PI}$. $I_{\rm PI0}$ is the initial peak noisy current, which is equal to

$$I_{\rm PI0} = (V_{IN} - V_{\rm CS0})/R_{\rm ds,PI}. \tag{4}$$

Here, $V_{\rm CS0}$ represents the initial voltage across $C_{\rm CS}$ in the state ON. The total $I_{\rm IN}$ equals the sum of $I_{\rm PI}$ and $I_{\rm MH}$, where $I_{\rm MH}$ is the drain current of switch M_H. With the EI, the state ON is randomly triggered to add $I_{\rm PI}$ to an unpredictable $I_{\rm MH}$ as shown in Fig. 3(b). Therefore, the injected $I_{\rm PI}$ can be treated as random current noise, even if it follows a fixed exponential pattern. In the state OFF, M_H and $M_{\rm PI}$ stay off to avoid any power profile leakage. The inductor L is charged by $C_{\rm CS}$ with the turn-ON of $M_{\rm CR}$ and then it is discharged through M_L as nominal operation. Once $V_{\rm CS}$ reaches to a regulated valley $V_{\rm CSV}$, the state OFF ends and $V_{\rm CSV}$ is initialized as $V_{\rm CS0}$ in next switching cycle.

To estimate power overhead, it is critical to analyze power loss distribution in the recycled masking power stage. While charge sharing loss of $C_{\rm CS}$ is dominant in the state ON, conduction loss of switch ON-resistance causes major loss in the state OFF as the discharge of $C_{\rm CS}$ is limited by I_L. With an optimal sizing of $M_{\rm CR}$, power overhead is mainly caused by charge sharing loss of $C_{\rm CS}$, which can be computed as

$$P_{\rm LOSS} = C_{\rm CS} \times f_{\rm SW,PI} \times (V_{\rm IN} - V_{\rm CSV})^2/2. \tag{5}$$

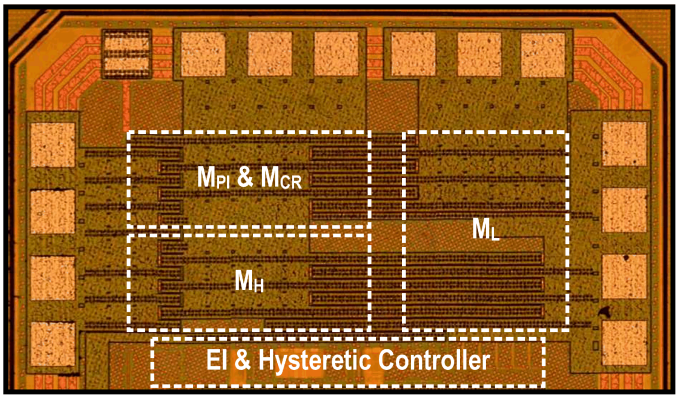


Fig. 7. Chip micrograph.

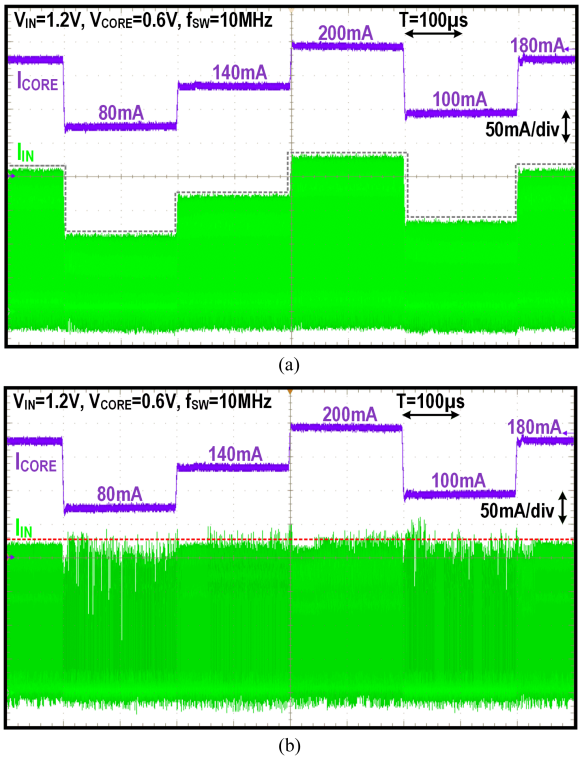


Fig. 8. Measured I_{IN} profile across dynamic I_{CORE} variations (a) without, and (b) with proposed random parallel power injection and charge recycling.

Here, V_{CSV} is the valley voltage across C_{CS} and $f_{SW,PI}$ is the f_{SW} of M_{PI}. Moreover, Fig. 3(b) shows that the encrypted power supply always maintains normal switching while only I_{IN} profile is manipulated by the recycled masking power stage. Thus, it only suffers negligible power and performance overhead caused by voltage difference between V_{IN} and V_{CSV}, which can be largely reduced by regulating V_{CSV} close to V_{IN}. Meanwhile, as indicated in (3) and (4), large I_{PI} can still be achieved with a smaller ON-resistance $R_{ds,PI}$ in M_{PI}. Therefore, system trade-offs among performance, power, and security are effectively mitigated.

B. Encryption Interface

Fig. 4(a) shows the circuit diagram of the EI. A ROT controller manages the operation states of main power stage and precisely regulates the valley voltage on C_{CS} at the reference voltage V_{CSV}. A valley modulator is used to adjust V_{CSV} to make it adaptive to I_{CORE} and thus calibrates the injected current noise for a constant I_{IN} profile. A switch logic uses digital gates to provide the clock signals for M_H, M_L, M_{PI}, and M_{CR}. Fig. 4(b) illustrates the operation timing diagram of the EI. Once V_{CS} is discharged to be lower than V_{CSV}, V_{RST} turns high and subsequently triggers V_{SEL} low. While the clock V_{CMP} is passed to V_{MH} and V_{ML}, V_{MPI}, and V_{MCR} remain low and high, respectively. The recycled masking power stage enters the state ON and charges V_{CS} by V_{IN}. After a random ON-timer provides a high V_{TON}, the state ON expires and the state OFF is activated by turning V_{SEL} high. V_{MH} and V_{MPI} stay high to shut down input power. V_{CMP} is passed to V_{MCR} and V_{ML} for power delivery. This continues until V_{CS} goes below V_{CSV} and the next switching cycle begins. Since the effective V_{TON} is randomly distributed, a ROT control is realized to encrypt I_{IN} profile successfully. In addition, if I_{CORE} varies, V_{CSV} is adaptively modulated to adjust the valley of V_{CS} and thus the injected power noise I_{PI} for a fixed I_{IN} profile. As shown in Fig. 4(b), increasing I_{CORE}, a lower switching node voltage V_{SW} is sensed to generate a higher V_{CSV} through a valley modulator and thus a smaller I_{PI2} is used for power injection. As the EI only regulates the capacitor C_{CS} without compromising main voltage regulation loop, system stability is strictly retained to achieve balanced system performance and security.

Fig. 5(a) depicts the circuit schematic of the random ON-timer, which is designed on the basis of the border-collision bifurcation [17]. Two currents I_1 and I_2 are utilized to charge and discharge a capacitor C_R, respectively, and make its voltage V_{CR} as a single chaotic variable. The SR-latch transitions V_{CR} from one state to the other for robust chaos, which is triggered by a comparator and a signal V_{CMP} from the hysteretic controller.

Its operation scheme is detailed in Fig. 5(b). In the switching cycle of $T_{SW}[n]$, V_{CR} is initialized as $V_{CR}[n]$, which is lower than the peak reference V_P. The rising edge of V_{CMP} resets the latch circuit and turns M_{PI} on. Thus, C_R is charged by I_1 as

$$V_{CR}\ (t) = V_{CR}\ [n] + (I_1 \times t)\,/C_R. \tag{6}$$

If V_{CR} crosses V_P within $T_{SW}[n]$, the comparator will set the latch and switch M_{N1} is turned on to discharge C_R. Accordingly, V_{CR} can be calculated as

$$V_{CR}\ (t) = V_P\ - (I_2 \times t)\,/C_R. \tag{7}$$

At the end of $T_{SW}[n]$, $V_{CR}[n+1]$ is computed as

$$V_{CR}\ [n+1] = V_P\ + k \times (V_P - V_{CR}\,[n]) - V_2, \tag{8}$$

where k is the ratio of I_2 to I_1 and V_2 is equal to $T_{SW} \times (I_2/C_R)$. On the contrary, if V_{CR} is always lower than V_P, C_R is continuously charged and $V_{CR}[n+1]$ equals

$$V_{CR}\ [n+1] = V_{CR}\ [n] + V_1, \tag{9}$$

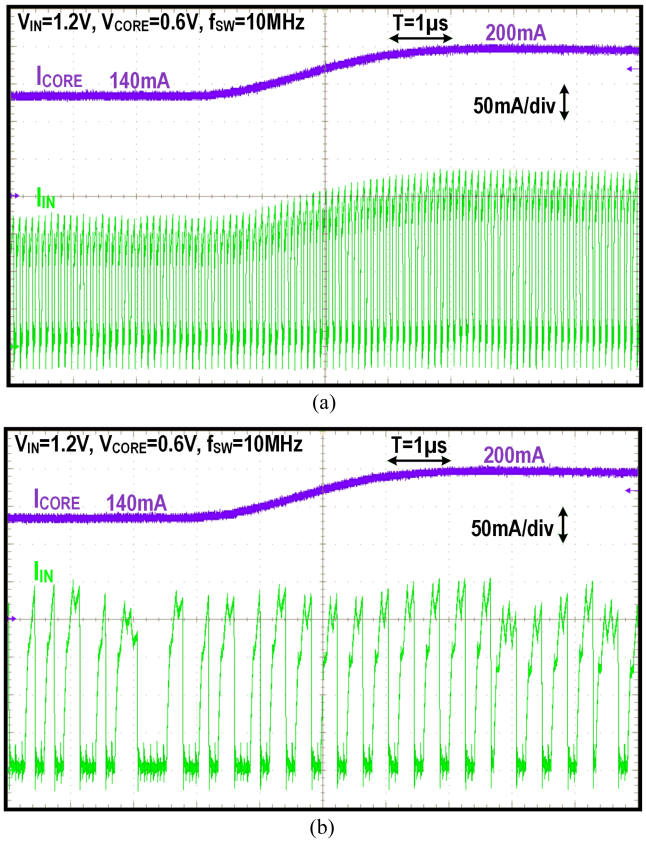


Fig. 9. Measured I_{IN} profile at I_{CORE} step-up (a) without, and (b) with proposed random parallel power injection and charge recycling.

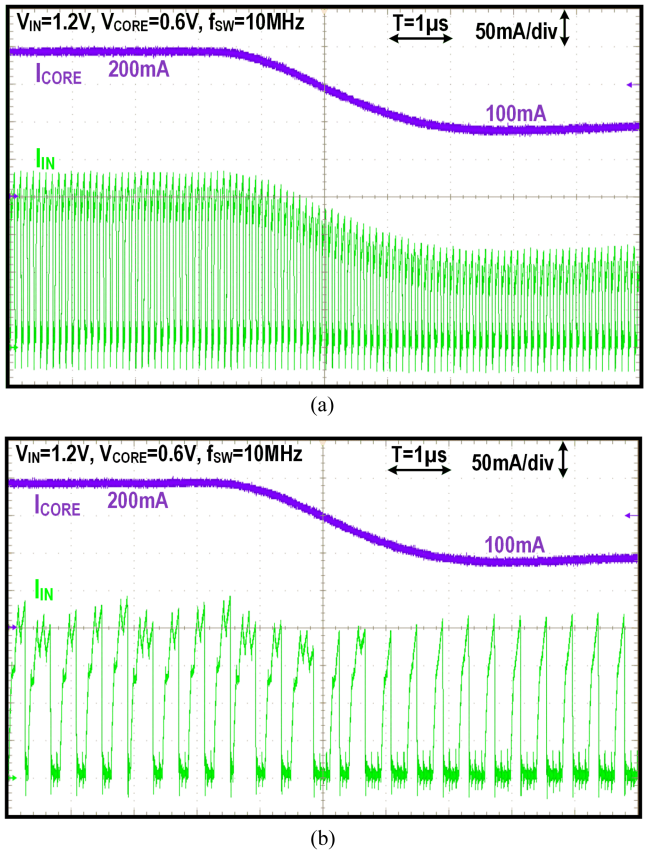


Fig. 10. Measured I_{IN} profile at I_{CORE} step-down (a) without, and (b) with proposed random parallel power injection and charge recycling.

where V_1 is equal to $T_{SW}\times(I_1/C_R)$. With these two cases, the one-dimensional chaotic map can be defined as

$$V_{CR}\ [n+1] = \begin{cases} V_P + k \times (V_P - V_{CR}\,[n]) - V_2, & V_{CR}\,[n] > V_B \\ V_{CR}\,[n] + V_1, & V_{CR}\,[n] \le V_B. \end{cases} \tag{10}$$

Here, V_B equals $(V_P - V_1)$ and represents the boundary case of $V_{CR}[n]$ at which $V_{CR}[n+1]$ equals V_P at the end of $T_{SW}[n]$. It has been proven that the dynamic map establishes chaos with proper design parameters of I_1, I_2, and V_P [18]. By sizing I_1 and I_2 small, the charge and discharge rates of C_R are greatly limited such that it takes longer than T_{SW} for V_{CR} to intersect with V_P and the discharge process ends with an unpredictable state. Thus, after skipping the effective V_{CMP}, V_{TON} is randomly triggered at a lower f_{SW} to define the T_{ON} for the proposed power stage. As such a chaotic map is independent of V_{IN}, it will keep random characteristics even if PIA manipulates V_{IN} aggressively.

The circuit implementation of the adaptive valley modulator is shown in Fig. 6. To monitor system power variations, V_{SW} is sensed by low V_{CMP} after a blanking time t_{BLK}. In the sensing period, the encrypted power supply connects V_{SW} to either V_{IN} or V_{CS} to deliver core power I_{CORE}. Although both V_{IN} and V_{CS} can be utilized for I_{CORE} detection, the use of V_{IN} protects the injected power noise I_{PI} from PIA. Thus, once V_{CMP} turns high, the difference between V_{SW} and V_{IN} is passed through a V-to-I circuit block and then converted to I_V, which is proportional to I_{CORE}. With a fixed biasing current I_B, V_{CSV} can be calculated as

$$V_{CSV} = V_{IN} - (I_B - I_V) \times R_{B2}, \tag{11}$$

where R_{B2} is a biasing resistor to set a proper V_{CSV}. If the state ON starts, V_{CS} is always initialized as its valley, which is equal to V_{CSV}. Therefore, combining the (3), (4), and (11), the injected noisy power I_{PI} is calculated as

$$I_{PI} = [(I_B - I_V) \times R_{B2}/R_{ds,PI}] \times e^{-t/R_{ds,PI}C_{CS}}, \tag{12}$$

which is independent of V_{IN} and adaptive to core power I_{CORE}. This feature makes the encrypted power supply resistant to PIA and helps secure system power profiles.

IV. Experimental Verification

The IC prototype of the proposed encrypted on-chip power supply is fabricated using a 65 nm CMOS silicon IC process. Fig. 7 shows the chip photograph, which has an active die area of only 0.19 mm^2. Power transistors are fully integrated on-chip with P-channel and N-channel MOSFETs to reduce gate drive complexity. Despite of using a hysteretic control, a fixed f_{SW} of 10 MHz is achieved by f_{SW} synchronization [16]. For system miniaturization, a 420 nH inductor L and a 1 μF output capacitor

TABLE I
PERFORMANCE COMPARISON

	JSSC 2018 [9]	JSSC 2020 [7]	TPEL 2020 [10]	This Work
Architecture	Inductive Regulator	Digital LDO	Inductive Regulator	Encrypted On-Chip Power Supply
Countermeasure Technique	Frequency Randomization	Supply Voltage Randomization	Frequency Randomization	Random Parallel Power Injection and Charge Recycling
Input Power Encryption	No	No	No	Yes
Process	130 nm CMOS	130 nm CMOS	55 nm CMOS	65 nm CMOS
Switching Frequency	Random	Not Reported	Random	Fixed
Security Target	Power SCA	Power/EM SCA	Power SCA and PIA	Power/EM SCA and PIA
Power Overhead	5%	32%	Not Reported	4.9%
Performance Overhead	3.33%	10.4%	Not Reported	0%*

* Performance overhead is estimated with design specifications of proposed power supply.

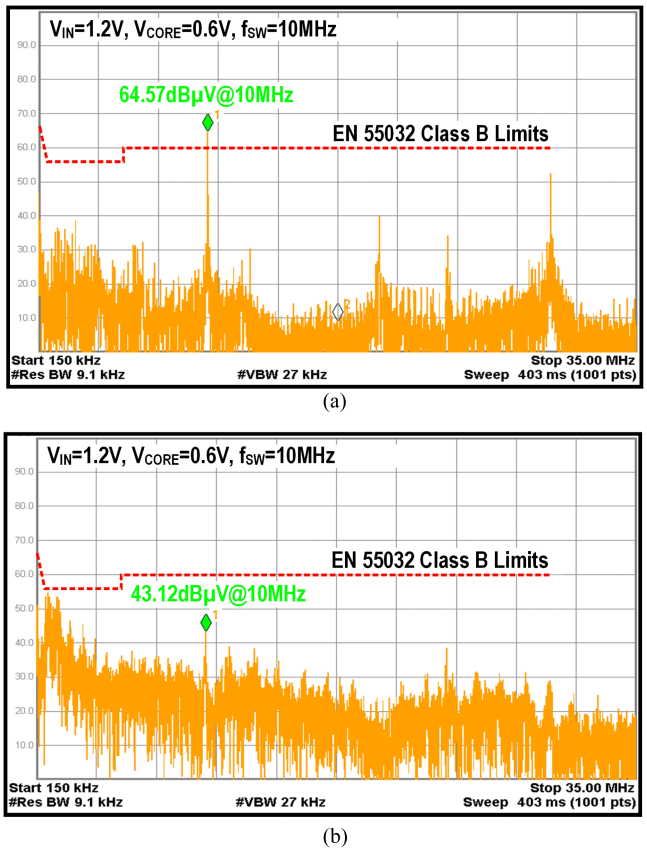


Fig. 11. Conducted EMI measurement at a I_{CORE} of 200 mA (a) without, and (b) with proposed random parallel power injection and charge recycling.

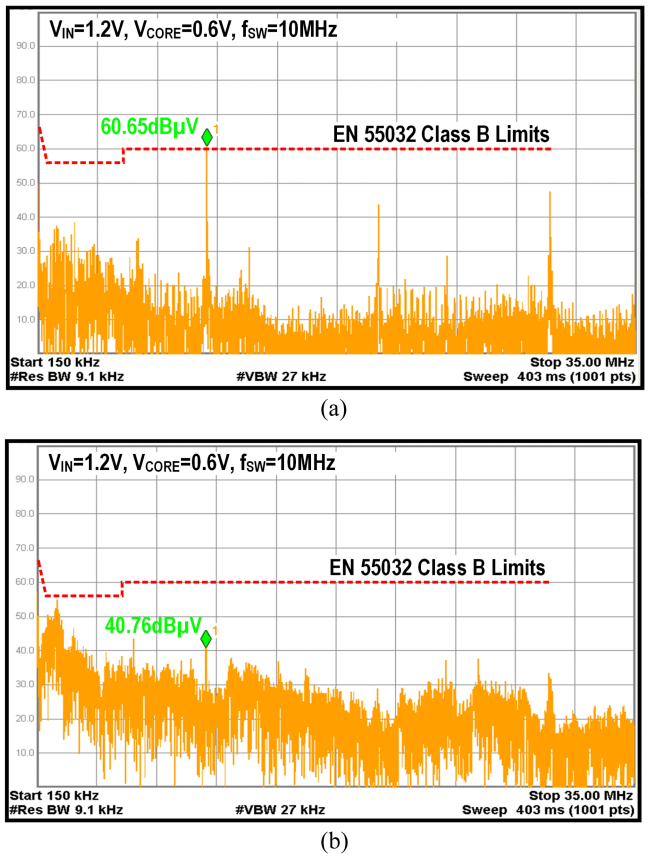


Fig. 12. Conducted EMI measurement at a I_{CORE} of 100 mA (a) without, and (b) with proposed random parallel power injection and charge recycling.

C_O are used on the power stage. Meanwhile, the flying capacitor C_{CS} is designed as 470 nF to support a maximum I_{CORE} of 200 mA. With a V_{IN} of 1.2 V, this power supply regulates core supply voltage V_{CORE} from 0.4 to 0.6 V efficiently.

To validate effective I_{IN} encryption of the presented power supply, Fig. 8 shows the measured I_{IN} profile across dynamic I_{CORE} variations. For a traditional switch mode power supply as shown in Fig. 8(a), I_{IN} profile follows the change of core power I_{CORE} immediately, making it vulnerable to PSCAs. Thanks to the recycled masking power stage, I_{IN} is fully encrypted by random power injection and charge recycling in Fig. 8(b), leading to a concealed "white noise" like I_{IN} profile despite of the same I_{CORE} activities as in Fig. 8(a). It thus greatly reduces the correlation between I_{IN} and I_{CORE} for high PSCA immunity. The detailed I_{IN} profile is measured in Fig. 9 as I_{CORE} steps up from 140 to 200 mA. The classic design in Fig. 9(a) leaks the highly correlated I_{IN} profile with a fixed f_{SW} of 10 MHz. However, Fig. 9(b) illustrates that this encrypted power supply effectively encrypts I_{IN} profile by noise injection, supply masking and switching randomization to protect I_{CORE}. Fig. 10 details the measured dynamic transient when I_{CORE}

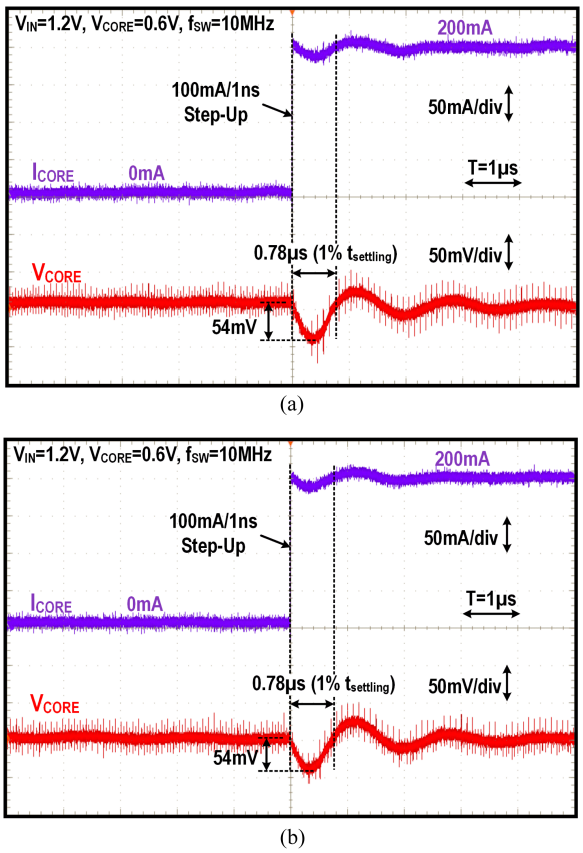


Fig. 13. Measured load step-up transient response (a) without, and (b) with proposed random parallel power injection and charge recycling.

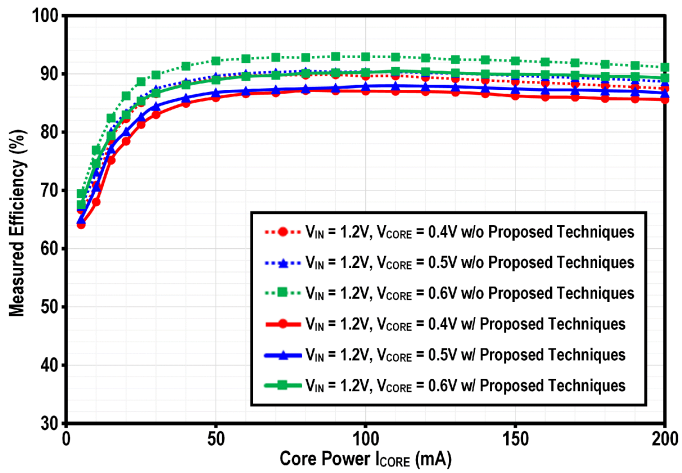


Fig. 14. Measured efficiency without and with proposed random parallel power injection and charge recycling.

steps down from 200 to 100 mA to verify consistent $I_{\rm IN}$ encryption. Thanks to the joint efforts of noise injection, supply masking, and switching frequency randomization, the real-time statistical correlation between $I_{\rm IN}$ and $I_{\rm CORE}$ is significantly reduced.

The conducted EMI is measured through a line impedance stabilization network and a spectrum analyzer. Fig. 11 depicts the measured conducted EMI noise spectra under a 1.2 V-to-0.6 V conversion with a $I_{\rm CORE}$ of 200 mA. If the parallel power injection and the charge recycling are disabled, the proposed power supply operates as a classic fixed frequency switching power supply. Hence, as shown in Fig. 11(a), it generates a peak EMI noise of 64.57 dBμV at the fundamental $f_{\rm SW}$ of 10 MHz, which exceeds the EN55032 Class B limits. With the random parallel power injection operation, the peak EMI noise is measured as 43.12 dBμV in Fig. 11(b), achieving 21.45 dB reduction to meet the EN55032 Class B limits and encrypt EM profile. Besides, most of EMI spectrum energy is transferred to a low frequency band from 150 kHz to 3.5 MHz and the measured noise floor is greatly increased by random parallel power injection and charge recycling operation. This reduces the SNR of input power profile and thus improve security against SCA as discussed in Section II. Fig. 12 shows the measured case at a $I_{\rm CORE}$ of 100 mA. The peak EMI noise is reduced from 60.65 dBμV to 40.76 dBμV to satisfy low EMI limits. Note that, this encrypted power supply only manipulates $I_{\rm IN}$ for low EMI and high SCA immunity while maintaining a fixed $f_{\rm SW}$ at 10 MHz. These merits simplify design requirements of system control loop and power components and mitigate the tradeoffs between security and power conversion in prior SCA countermeasures significantly.

Fig. 13 shows the measured load transient response to verify performance overhead of this design. In response to $I_{\rm CORE}$ step-up from zero to full power of 200 mA, the encrypted power supply achieves the $V_{\rm CORE}$ droop of 54 mV with 1% settling time $t_{settling}$ of 0.78 μs, which is the same as the measured results without random parallel power injection and charge recycling. Accordingly, performance overhead turns out to be negligible.

Fig. 14 provides the measured data on the circuit efficiencies with and without proposed techniques. Operating in continuous conduction mode, the encrypted power supply achieves 90.5% peak efficiency at a $I_{\rm CORE}$ of 110 mA in the 1.2 V-to-0.6 V conversion. Thanks to the efficient charge recycling, the maximum power overhead is limited to 4.9%.

Finally, Table I shows the comparison of this work with the prior arts. While existing solutions directly apply randomization to power circuits, the proposed power supply utilizes the parallel structure to achieve power encryption without affecting power delivery. Moreover, as a more comprehensive scheme, random parallel power injection and charge recycling are implemented to simultaneously accomplish noise injection, supply masking and switching randomization to improve side-channel security. Instead of randomizing entire system operation, this design can operate at a fixed $f_{\rm SW}$ while only encrypt $I_{\rm IN}$ profiles, which is the root cause of PSCA. The peak EMI noise is attenuated to improve security against EM SCA with the minimal power and performance overhead.

V. Conclusion

An encrypted on-chip power supply is presented in this article as the SCA countermeasure to enhance hardware security. Thanks to random parallel power injection and charge recycling, this power supply effectively encrypts both input power

profile and EM profile with noise injection, supply masking and switching randomization. To achieve such, a recycled masking power stage is implemented to inject noisy power and recycle charge in parallel of nominal power delivery. An EI manages the operations of power delivery and security with precise regulation of the parallel input branch under ROT modulation. This enables adaptive power injection and switching randomization to maintain consistent input power encryption and thus mask core power variations. Performance and power overheads are significantly reduced with parallel power encryption to mitigate design conflicts between power and security. The experimental results successfully verify this design.

REFERENCES

[1] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *J. Cryptograph. Eng.*, vol. 1, no. 1, pp. 5–27, Apr. 2011.

[2] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Aug. 2004, pp. 16–29.

[3] D. Canright and L. Batina, "A very compact 'perfectly masked' sbox for AES," in *Proc. 6th Int. Conf. Appl. Cryptogr. Netw. Secur.*, New York, NY, Jun. 2008, pp. 446–459.

[4] J. D. Golic and C. Tymen, "Multiplicative masking and power analysis of AES," in *Proc. 4th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Redwood Shores, CA, USA, Aug. 2002, pp. 198–212.

[5] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. 8th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Yokohama, Japan, Oct. 2006, pp. 232–241.

[6] D. Hwang et al., "AES-based security coprocessor IC in 0.18μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[7] A. Singh et al., "Enhanced power and electromagnetic SCA resistance of encryption engines via a security-aware integrated all-digital LDO," *IEEE J. Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, Feb. 2020.

[8] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 4, no. 2, pp. 169–179, Jun. 2014.

[9] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, Aug. 2018.

[10] W. Yang et al., "A true-random-number-based pseudohysteresis controller for buck DC–DC converter in high-security Internet-of-Everything devices," *IEEE Trans. Power Electron.*, vol. 35, no. 3, pp. 2969–2978, Mar. 2020.

[11] J. Longo, E. De Mulder, D. Page, and M. Tunstall, "SoC it to EM: Electromagnetic side-channel attacks on a complex system-on-chip," in *Proc. 17th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Saint-Malo, France, Sep. 2015, pp. 620–640.

[12] D. Das et al., "EM and power SCA-resilient AES-256 through >350× current-domain signature attenuation and local lower metal routing," *IEEE J. Solid-State Circuits*, vol. 56, no. 1, pp. 136–150, Jan. 2021.

[13] T. Güneysu and A. Moradi, "Generic side-channel countermeasures for reconfigurable devices," in *Proc. 13th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Nara, Japan, Sep. 2011, pp. 33–48.

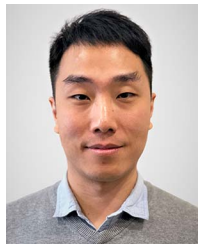
[14] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Proc. 2nd Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Worcester, MA, Aug. 2000, pp. 71–77.

[15] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.

[16] K. Wei and D. B. Ma, "A 10-MHz DAB hysteretic control switching power converter for 5G IoT power delivery," *IEEE J. Solid-State Circuits*, vol. 56, no. 7, pp. 2113–2122, Jul. 2021.

[17] T. Kousaka et al., "Analysis of border-collision bifurcation in a simple circuit," in *Proc. IEEE Int. Symp. Circuits Syst.*, Geneva, Switzerland, May 2000, pp. 481–484.

[18] S. Mandal and S. Banerjee, "Analysis and CMOS implementation of a chaos-based communication system," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 51, no. 9, pp. 1708–1722, Sep. 2004.



Kang Wei (Member, IEEE) received the B.E. degree in microelectronics from Northwestern Polytechnical University, Xi'an, China, in 2011, and the Ph.D. degree in electrical engineering from the University of Texas at Dallas, Richardson, TX, USA, in 2021.

From 2011 to 2013, he worked as a Research Assistant with Sun Yat-sen University, Guangzhou, China, focusing on the design of analog circuits and system for Lock-in amplifier. He joined Texas Instruments, Dallas, TX, in 2016 and 2017, respectively, as an Analog Design Intern, working on highly efficient point-to-load power IC design. Since 2021, he has been an Analog Design Engineer with Kilby Labs at Texas Instruments, Dallas, TX, USA, where he is currently developing high-voltage gate drivers, galvanic isolation solutions and ultra-low-cost linear regulators for automotive, industrial and consumer power systems.

Jin Woong Kwak (Student Member, IEEE) received the B.S. degree in electrical engineering from the University of Texas at Dallas, in 2017. He is currently working toward the Ph.D. degree in electrical engineering from the University of Texas at Dallas, Richardson, TX, USA.

In 2017, he worked as an undergraduate Research Assistant with the University of Texas at Dallas, focusing on the analysis and design of spin-torque transfer magnetic random-access memory (STT-MRAM). His current research interests include hybrid converter topologies, power management IC design for high step-down dc–dc conversion and point-of-load applications.

D. Brian Ma (Senior Member, IEEE) received the B. S. and the M. S. degrees in electronic science from NanKai University, Tianjin, China, in 1995 and 1998, respectively, and the Ph. D. degree in electrical and electronic engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2003.

He was a faculty member with Louisiana State University, Baton Rouge, LA, and then the University of Arizona, Tucson, AZ. He is currently the Distinguished Chair in Microelectronics and a Full Professor with the Department of Electrical and Computer Engineering, University of Texas at Dallas, Richardson, TX, USA. He has authored or coauthored more than 180 peer-reviewed journal and conference papers and 5 book and book chapters on these subjects. He also delivered over 130 invited talks, education tutorials and presentations in prominent conference and industry venues. His research focuses on integrated power electronics, with primary interests on power circuit control and operation, wide bandgap (WBG) power electronics, power device and circuit reliability, aging and security, and artificial intelligence driven smart power systems.

Prof. Ma is also the Director of Integrated Power System Laboratory at the university. He has served on the Executive Committee of Semiconductor Research Corporation (SRC) Texas Analog Center of Excellence (TxACE), since 2010 and was the Lead of Energy Efficiency thrust between 2010 and 2018. He was also the director of Texas Instruments Foundational Technology Research Center on Power Density from 2018 to 2021. Along his professional career path, He was honored with Analog Devices Professorship (2004–2008), TxACE Distinguished Chair (2010–2012), Erik Jonsson Distinguished Chair (2012–2017) and Distinguished Chair in Microelectronics (2017-present). He also received the University of Arizona AAFSAA Outstanding Faculty Award in 2006, and was a finalist for University of Arizona Accolades Outstanding Faculty Award in 2009. His research works have been sponsored by the U.S. federal agencies including National Science Foundation, Semiconductor Research Corporation and DARPA and numerous leading semiconductor companies. He was a recipient of United States National Science Foundation CAREER Award in 2009. He was also the recipient or co-recipient of numerous technical awards from international conferences and journals.