Time-Delayed Converter-Reshuffling: An Efficient and Secure Power Delivery Architecture

Weize Yu and Selçuk Köse, *Member, IEEE*

***Abstract*—In this letter, a time-delayed converter-reshuffling (CoRe) technique is proposed as a countermeasure against machine learning based differential power analysis (DPA) attacks where the attacker can synchronize the sampling frequency with the operating frequency of the device under attack. The proposed time-delayed CoRe technique exploits the distributed nature of multiphase switched capacitor voltage converters where half of the converter stages are delayed to eliminate the risk of having zero power trace entropy (PTE) under machine learning based DPA attacks. A high PTE value is maintained (above 3.2 for a 64-phase time-delayed CoRe technique) regardless of the phase difference between the attacker's sampling rate and the operating frequency. In addition, the minimum PTE value of the proposed time-delayed CoRe technique is enhanced from zero to $\sim$ 3 by inserting a certain time-delay to half of the converter stages.**

***Index Terms*—Machine learning-based DPA attacks, multiphase switched capacitor, power trace entropy, time-delayed.**

I. Introduction

SIDE-CHANNEL ATTACKS (SCA) are powerful noninvasive attacks which can be used to obtain the secret key in a cryptographic circuit in feasible time without the need for expensive measurement equipment. Differential power analysis (DPA) attacks are a type of SCA that exploit the correlation between leaked power consumption information and the processed/stored data [1]. Although several methods [2]–[4] have been proposed as a countermeasure against DPA attacks, significant power overhead needs to be wasted to minimize the information leakage through the side-channels.

Converter-gating (CoGa) has recently been proposed [5] to minimize the information leakage while maintaining high power conversion efficiency. A multiphase switched capacitor (SC) voltage converter is used in CoGa where certain converter stages are adaptively activated and gated based on the workload. In the CoGa technique, each individual converter stage is forced to operate near the peak efficiency. Since CoGa utilizes SC voltage converters that charge and discharge within every switching cycle, the average input power of the converter within a switch period highly correlates with the average output power. Additionally, since the input clock signals that control the switches within each converter stage have a certain phase shift, the spikes in the input current profile of different stages also exhibit varying time shifts. A timing uncertainty can therefore be introduced in the monitored power profile when a pseudo-random number generator (PRNG) is utilized to scramble the activation pattern of the CoGa technique [5].

Recently, a workload-agnostic converter-reshuffling (CoRe) technique has been proposed to randomly activate and deactivate converter stages to scramble the power consumption profile with a PRNG [6]. The main drawback of the conventional CoRe technique in [6] is that the attacker can obtain switching frequency f_s and phase information with machine learning attacks. If the attacker can synchronize the attack with the switching frequency of the on-chip SC converter, the average power within a switching period would leak critical information to the attacker that may annihilate the added security benefit of reshuffling the converter stages.

In this letter, a new technique, *time-delayed CoRe*, is introduced to cope with machine learning-based DPA attacks. In the proposed time-delayed CoRe technique, half of converter stages are delayed with a certain time-shift, eliminating possible synchronization of the attacker's sampling frequency with the switching frequency of the converter. With this technique, the minimum PTE value is significantly increased as compared to the conventional CoRe technique [6] under machine learning attacks even when the attacker's sampling frequency is in complete synchronization with the SC voltage converter.

II. Modeling

Entropy is commonly used in information theory to model the level of uncertainty (or randomness) in a given data set. In cryptography, entropy is used to evaluate the security performance of integrated systems against SCA [7], [8]. We will use entropy to quantify the security performance of different on-chip voltage converters. The input power of a voltage converter $H_i(t), (i = 1, 2, \ldots, k)$ can have k different values while delivering the same output power $P_{out}(t)$ to the load circuits depending on the design parameters of the voltage converter and the phase and frequency of the input switching signal. Let's assume that the probability of having different input power values is $p_i(t), (i = 1, 2, \ldots, k)$. The input power trace entropy $PTE(t)$ of a voltage converter can then be defined as

$$PTE(t) = -\sum_{i=1}^{k} p_i(t) log_2^{p_i(t)}. \quad (1)$$

A. Converter-Reshuffling (CoRe) Technique

Primarily, two parameters of an on-chip SC converter can leak the load power information to attackers: switching frequency and number of active converter stages. The switching

Manuscript received April 03, 2015; accepted May 09, 2015. Date of publication May 13, 2015; date of current version August 27, 2015. This work was supported in part by the National Science Foundation CAREER Award under Grant CCF-1350451 and by the USF Presidential Fellowship. This manuscript was recommended for publication by Z. Shao.

The authors are with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: weizeyu@mail.usf.edu; kose@usf.edu).

Color versions of one or more of the figures in this letter are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/LES.2015.2433175

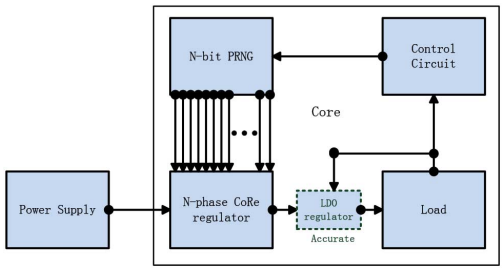

Fig. 1. Schematic of the CoRe technique [6].

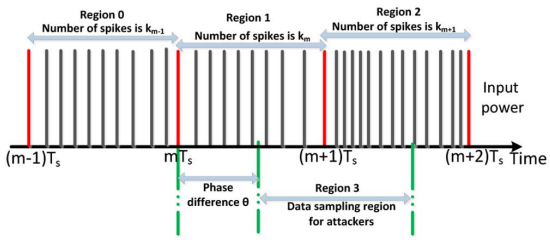

Fig. 2. Input power profile of the CoRe technique.

frequency f_s has a monotonic relationship with the output power P_{out} [9]. f_s is therefore fixed in this letter to eliminate possible leakage of the workload information. The number of active converter stages increases with the workload and therefore may leak the workload information to the attacker.

A system level architecture of the CoRe technique is illustrated in Fig. 1. The output power resolution N/P_{out} at the output of SC converter can be degraded while using a fixed-frequency modulation if the number of phases N is small. A low-dropout (LDO) regulator can be inserted at the output of the SC converter to mitigate the possible output DC shift. If the number of phases N is sufficiently large, the CoRe technique has a fine output power resolution and the LDO regulator can be removed.

The input power of the CoRe technique, which may be monitored by an attacker, is illustrated in Fig. 2. f_s and T_s are, respectively, the switching frequency and period. The number of spikes in regions 0, 1, and 2 are, respectively, k_{m-1}, k_m, and k_{m+1}. The phase difference between switching frequency and data sampling by the attacker is θ and the power consumption at each converter stage is P_0. To represent the input power information between mT_s and $(m+2)T_s$, an array A_m is defined as

$$A_m = [a_{m,1}, \ldots, a_{m,N}, a_{m,(N+1)}, \ldots, a_{m,2N}]P_0 \quad (2)$$

where $\sum_{i=1}^{N} a_{m,i} = k_m$, $\sum_{i=N+1}^{2N} a_{m,i} = k_{m+1}$, and $a_{m,i} \in \{0,1\}, (i = 1,2,\ldots,2N)$. We define another array $H_m = [h_1, h_2, \ldots, h_{2N}]$ to represent the monitored power data by the attacker within a switching period with the values h_i as

$$h_i = \begin{cases} 0 & ,i \le [\theta/360{*}N] \\ 1 & ,[\theta/360{*}N] < i \le [\theta/360{*}N] + N \\ 0 & ,i > [\theta/360{*}N] + N. \end{cases} \quad (3)$$

The input power data $P_{s,m}$ sampled by an attacker within a switch period can then be written as

$$P_{s,m} = A_m H_m^T. \quad (4)$$

The next step is to enumerate all of the possible arrays A_m and count the number of each sampled power $P_{s,m}$. If the frequency for all the possible sampled power data $P_{s,m}$ is

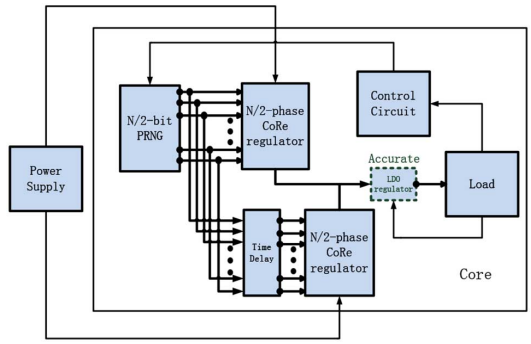

Fig. 3. Schematic of the proposed time-delayed CoRe technique with an $N/2$-bit PRNG.

$g_j(\theta, k_m, k_{m+1}), (j = 1,2,\ldots,D)$ where D is the total number of possible sampled input power data, the corresponding probability $\beta_j(\theta, k_m, k_{m+1}), (j = 1,2,\ldots,D)$ is

$$\beta_j(\theta, k_m, k_{m+1}) = \frac{g_j(\theta, k_m, k_{m+1})}{\binom{N}{k_m}\binom{N}{k_{m+1}}}. \quad (5)$$

The PTE value of CoRe technique PTE_1 can be written as

$$PTE_1 = -\sum_{j=1}^{D} \frac{g_j(\theta, k_m, k_{m+1})}{\binom{N}{k_m}\binom{N}{k_{m+1}}} log_2 \frac{g_j(\theta, k_m, k_{m+1})}{\binom{N}{k_m}\binom{N}{k_{m+1}}}. \quad (6)$$

To synchronize the attack with the frequency of the voltage converter, an attacker can enter a constant input data to the circuit. Under a constant input sequence, the leakage power consumption within any switching cycle monitored at the input of the CoRe technique would be constant ($k_m = k_{m+1} = \ldots$). By analyzing the power profile with machine learning attacks, the attacker can acquire the switching frequency f_s and synchronize the attack to have $\theta = 0^\circ$. PTE value of CoRe technique becomes zero when the phase difference $\theta = 0^\circ$ or 360°, as shown in Fig. 6. The proposed time-delayed CoRe technique provides an enhanced protection by maintaining high PTE under machine learning attacks.

B. Time-delayed Converter-Reshuffling (CoRe) Technique

A time-delayed CoRe technique is proposed to scramble the monitored power consumption so that an attacker will no longer extract meaningful information from the side-channel leakage. In this technique, half of the converter stages in the CoRe scheme will be activated and gated with a time delay, as shown in Fig. 3. An $N/2$-bit PRNG is used to generate the gate signal.

An array B_m is defined to represent the input power information from $(m-1)T_s$ to $(m+2)T_s$, as shown in Fig. 4, as

$$B_m = [b_{(m-1),1}, \ldots, b_{(m-1),N/2}, b_{(m-1),N/2+1}, \ldots, b_{(m-1),N}, b_{(m-1),N+1}, \ldots, b_{(m-1),3N/2}]P_0 \quad (7)$$

where $b_{(m-1),i} \in \{0,1\}, (i = 1,2,\ldots,3N/2)$ and

$$\left[\sum_{i=1}^{N/2} b_{(m-1),i}, \sum_{i=N/2+1}^{N} b_{(m-1),i}, \sum_{i=N+1}^{3N/2} b_{(m-1),i}\right] = [k_{m-1}/2, k_m/2, k_{m+1}/2]. \quad (8)$$

In time-delayed CoRe, instead of H_m, there are two different arrays $Z_m = [z_1, z_2, \ldots, z_{3N/2}]$ and $W_m = [w_1, w_2, \ldots, w_{3N/2}]$ which represent, respectively, the power data monitored by an attacker from the conventional $N/2$ phases and time-delayed $N/2$ phases. z_i and w_i can be written as

$$z_i = \begin{cases} 0 & , i \le [(\theta/360)*(N/2)] + N/2 \\ 1 & , \left[\frac{\theta}{360}*\frac{N}{2}\right] + \frac{N}{2} < i \le \left[\frac{\theta}{360}*\frac{N}{2}\right] + N \\ 0 & , i > [(\theta/360)*(N/2)] + N, \end{cases} \quad (9)$$

$$w_i = \begin{cases} 0 & , i \le [((\theta-\alpha)/360)*(N/2)] + N/2 \\ 1 & , \left[\frac{(\theta-\alpha)}{360}*\frac{N}{2}\right] + \frac{N}{2} < i \le \left[\frac{(\theta-\alpha)}{360}*\frac{N}{2}\right] + N \\ 0 & , i > [((\theta-\alpha)/360)*(N/2)] + N \end{cases} \quad (10)$$

where $\alpha = (T_0/T_s) * 360^\circ$ is the delayed phase angle and T_0 is the time delay. The input power data $P'_{s,m}$ of time-delayed CoRe that is monitored by an attacker within a switch period becomes

$$P'_{s,m} = B_m Z_m^T + B_m W_m^T. \quad (11)$$

The next step is to execute all the possible arrays B_m and count the number of each sampled power $P'_{s,m}$. If the number of all possible sampled input power data is $x_j(\theta, k_{m-1}, k_m, k_{m+1}), (j = 1, 2, \ldots, E)$ where E is the total number of possible sampled input power data, then the probability $\gamma_j(\theta, k_{m-1}, k_m, k_{m+1}), (j = 1, 2, \ldots, E)$ for all the possible input power data $P'_{s,m}$ sampled by the attacker is

$$\gamma_j(\theta, k_{m-1}, k_m, k_{m+1}) = \frac{x_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N/2}{k_{m-1}/2}\binom{N/2}{k_m/2}\binom{N/2}{k_{m+1}/2}}. \quad (12)$$

The input power trace entropy PTE_2 for time-delayed CoRe technique with an $N/2$-bit PRNG therefore becomes

$$PTE_2 = -\sum_{j=1}^{E} \gamma_j(\theta, k_{m-1}, k_m, k_{m+1}) log_2^{\gamma_j(\theta, k_{m-1}, k_m, k_{m+1})}. \quad (13)$$

To investigate the effect of the PRNG bit length on the entropy level, an N-bit PRNG is used, as shown in Fig. 5, as compared to the $N/2$-bit PRNG, as shown in Fig. 3. C'_m and C''_m arrays are defined to represent the input power information of normal phases and time-delayed phases from $(m-1)T_s$ to $(m+2)T_s$, as shown in Fig. 4, and can be written as

$$C'_m = [c'_{(m-1),1}, \ldots, c'_{(m-1),N/2}, c'_{(m-1),N/2+1}, \ldots, c'_{(m-1),N}, c'_{(m-1),N+1}, \ldots, c'_{(m-1),3N/2}]P_0, \quad (14)$$

$$C''_m = [c''_{(m-1),1}, \ldots, c''_{(m-1),N/2}, c''_{(m-1),N/2+1}, \ldots, c''_{(m-1),N}, c''_{(m-1),N+1}, \ldots, c''_{(m-1),3N/2}]P_0 \quad (15)$$

where $c'_{(m-1),i}, c''_{(m-1),i} \in \{0, 1\}, (i = 1, 2, \ldots, 3N/2)$, and

$$\left[\sum_{i=1}^{N/2}(c'_{(m-1),i} + c''_{(m-1),i}), \sum_{i=N/2+1}^{N}(c'_{(m-1),i} + c''_{(m-1),i}), \sum_{i=N+1}^{3N/2}(c'_{(m-1),i} + c''_{(m-1),i})\right] = [k_{m-1}, k_m, k_{m+1}]. \quad (16)$$

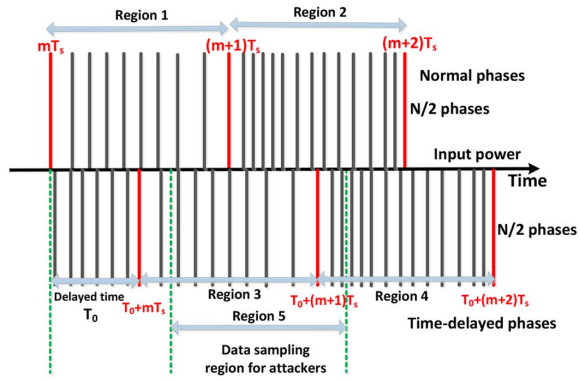

Fig. 4. Input power of the time-delayed CoRe technique.

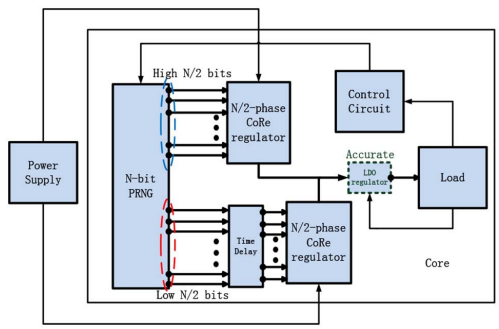

Fig. 5. Schematic of the proposed time-delayed CoRe technique with an N-bit PRNG.

The input power data $P''_{s,m}$ of time-delayed CoRe with N-bit PRNG monitored by an attacker within a switching period is

$$P''_{s,m} = C'_m Z_m^T + C''_m W_m^T. \quad (17)$$

When all possible values of C'_m and C''_m are listed, the frequency $y_j(\theta, k_{m-1}, k_m, k_{m+1}), (j = 1, 2, \ldots, F)$ for each sampled power $P''_{s,m}$ can be determined, where F is the total number of possible sampled input power data. So the corresponding probability $\lambda_j(\theta, k_{m-1}, k_m, k_{m+1}), (j = 1, 2, \ldots, F)$ is

$$\lambda_j(\theta, k_{m-1}, k_m, k_{m+1}) = \frac{y_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N}{k_{m-1}}\binom{N}{k_m}\binom{N}{k_{m+1}}}. \quad (18)$$

The input power trace entropy PTE_3 for time-delayed CoRe technique with an N-bit PRNG is

$$PTE_3 = -\sum_{j=1}^{F} \frac{y_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N}{k_{m-1}}\binom{N}{k_m}\binom{N}{k_{m+1}}} log_2^{\frac{y_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N}{k_{m-1}}\binom{N}{k_m}\binom{N}{k_{m+1}}}}. \quad (19)$$

III. Results and Discussions

The PTE value for the CoRe technique with a 64 bit PRNG and for time-delayed CoRe technique with 32 and 64 bit PRNGs are shown in Fig. 6 when the output power dissipation changes from $(N/2)*\eta P_0$ to $(3N/4)*\eta P_0$. Here, $N = 64$ and η is the power efficiency. The PTE value for CoRe technique becomes zero when the phase difference θ between switching frequency

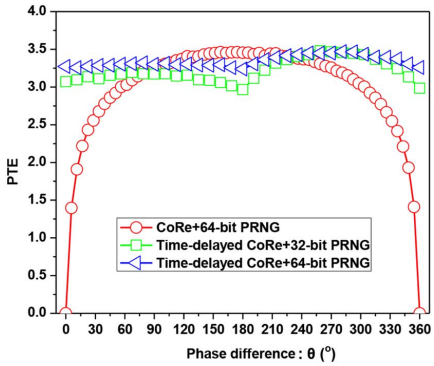

Fig. 6. PTE value versus the phase difference between switching frequency and data sampling frequency (time delay $T_0 = T_s/2$).

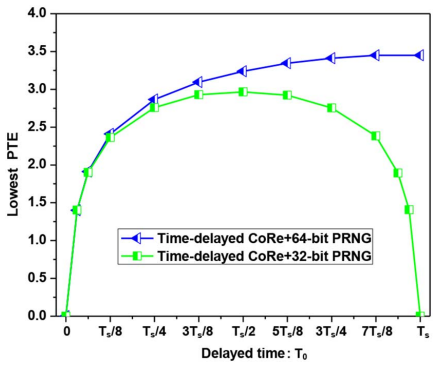

Fig. 7. Lowest PTE value versus the time delay.

and data sampling frequency is 0° or 360°. In this case, the CoRe technique fails to provide any additional security against DPA attacks if machine learning attacks are applied. However, the time-delayed CoRe technique continuously demonstrates high PTE values (above 3.2) all the time for $0° < \theta < 360°$. Even if the machine learning based DPA attacks can determine the activation/deactivation pattern and synchronize the attack with the voltage converter, there still exists a high amount of uncertainty in the monitored data for an attacker to achieve a successful attack. This uncertainty is due to the withholding of charge in some of the converter stages independent of the activation/deactivation pattern. The number of spikes in each switching cycle therefore becomes independent of the workload information and the activation pattern in the proposed technique.

The optimum time delay for the proposed time-delayed CoRe with 32-bit PRNG is $\sim T_s/2$, as shown in Fig. 7. The PTE value of the time-delayed CoRe with a 32-bit PRNG, however, becomes zero when the time difference is either zero or a full period. As shown in Fig. 7, the PTE value for the time delayed CoRe with a 64-bit PRNG increases monotonically with the time delay since both of the $N/2$ converter stages are controlled by different bits of the PRNG. In a practical design, the selection of time delay T_0 also needs to satisfy $T_0 = n*(\frac{2T_s}{N}), (n = 1, 2, \ldots, N/2)$ to prevent the attacker from splitting the power information of normal phases and time-delayed phases.

When the total number of phases N increases, the lowest PTE value of CoRe technique always maintains at zero while the lowest PTE value of the proposed time-delayed CoRe technique

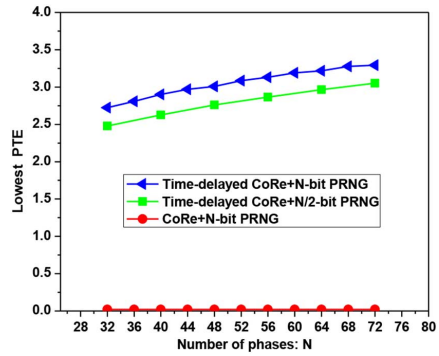

Fig. 8. Lowest PTE value versus the number of phases ($T_0 = T_s/2$).

monotonically increases due to higher PRNG entropy, as shown in Fig. 8. Time-delayed CoRe technique therefore becomes a more effective countermeasure against machine learning based DPA attacks with greater number of converter stages.

Please note that the proposed time-delayed CoRe technique only requires one additional circuitry that performs the time delay operation. The area overhead is therefore quite negligible (*i.e.,* less than 1%) as compared to the conventional CoRe technique.

IV. Conclusion

The conventional CoRe technique is vulnerable under machine learning based DPA attacks if the attacker synchronizes the attack with the switching frequency of the on-chip voltage converter. Time-delayed CoRe technique delays half of the converter stages, making it infeasible to synchronize the attack with the switching frequency. An analytical expression for the PTE is developed to evaluate the security-performance of the conventional and time-delayed CoRe techniques. The lowest PTE value of the time-delayed CoRe technique is enhanced significantly even under machine learning based DPA attacks.

References

[1] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks Revealing the Secrets of Smart Cards (Advances in Information Security)*. Berlin, Germany: Springer-Verlag, 2007.

[2] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 3, pp. 23–31, Jan. 2010.

[3] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," *VLSI Design*, pp. 854–862, Jan. 2007.

[4] D. Wu, X. Cui, W. Wei, R. Li, D. Yu, and X. Cui, "Research on circuit level countermeasures for differential power analysis attacks," *Solid-State Integr. Circuit Technol. (ICSICT)*, pp. 1–3, 2012.

[5] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 4, no. 7, pp. 169–179, Jun. 2014.

[6] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *Proc. IEEE/ACM Design Autom.Conference (DAC)*, Jun. 2015.

[7] B. Kopf and D. Basin, "An information-theoretic model for adaptive side-channel attacks," *CCS*, pp. 286–296, 2007.

[8] H. Maghrebi, S. Guilley, J. L. Danger, and F. Flament, "Entropy-based power attack," *Hardware-Oriented Security Trust (HOST)*, pp. 1–6, Jun. 2010.

[9] T. M. Andersen *et al.*, "A 4.6 W/mm² power density 86% efficiency on-chip switched capacitor DC-DC converter in 32 nm SOI CMOS," in *Proc. IEEE Int. Appl. Power Electron. Conf. Exposition*, Mar. 2013, pp. 692–699.