Enhanced Measurement And Evaluation Of Power Analysis Attacks On Asynchronous S-Box

[1] M.R.Shri suvega,
PG Scholar, Akshaya College of engineering and technology,
Coimbatore, India.
shrisuvega91@gmail.com

[2] P.Niranjana Devi,
PG Scholar, Akshaya College of engineering and technology,
Coimbatore, India.
p.niranjanadevi@gmail.com

***Abstract*— In this work,a novel asynchronous combinational S-Box (substitution box) design for AES(Advanced Encryption Standard) cryptosystems is proposed and validated.The S-Box is examined as the ultimate critical component in AES crypto-circuits since it employ the most power and leaks the most information contrary to side-channel attacks.The prospective design is based on a unresponsive logic paradigm known as Null Conventional Logic (NCL).The proposed NCL S-Box provides vast benefits over existing designs since it consumes less power therefore suited for energy constraint mobile crypto-utilizations.It also emanates less noise and has grace power peaks therefore leaks less information against side-channel attacks such as differential power/noise analysis.Functional verification and power measurement of NCL S-Box have been done using Mentor Graphics EDA (Electronic Design Automation) tool to assure low-power side-channel attack-resistant operation of the proposed clock-free AES S-Box design.**

Keywords- *Advanced Encryption Standard (AES); Null Convention Logic (NCL); Power measurement; Substitution Box(S-Box)*

I. INTRODUCTION

Most modern cryptographic devices are employed using semiconductor logic gates,which are constructed out of transistors.The impending of the cryptohardware devices and its algorithms are a framework of modern digital information systems which handles the crisis for data security,authentication and unsusceptible information.The cryptohardware is exposed to plenty of attacks which precise the physical properties of their aiding.Security is materialized as a development of chief importance.This is the particular truth for the embedded system due to several clear cut security challenges.Cryptography is the best and sufficient solution for these challenges which counterclaims to encode digital information while being energy efficient are in high demand.The novelty for such devices are accessible in today's mobile phones,portable devices and network security. The aim to reach this demand of low-power devices with development security features,researchers examine the cryptographic algorithm.The cryptographic algorithm transforms plain text information into cipher text with additional secret cipher key.The algorithm is an expansion way to inspect the plain text from cipher text without the explicit knowledge of the cipher key.The security furnished by the algorithm is equal to its capacity to safe the cipher key.The cryptosystems output incorporate execution timing,power consumption,electromagnetic leaks and also thermal or acoustic emancipation.All these information sources are known as side channels.Such side channel attack exploit power consumption of the device during prediction to derive the secret key.These side channel attacks are known as Differential Power Analysis (DPA) attacks.Among side channels attacks DPA is maximum dominant.DPA attack can mention secret keys through numerically analyzing power consumption measurements from a cryptosystems.Typically to do the DPA attack,the attackers follows the consecutive steps, (1) Gather the power consumption analysis from the encrypted device with irregular inputs. (2) Arrange the collected results by using decision function. (3) Revise the step (1) with a hypothetical key. (4) Sort the results to the existing sets. (5) Do the average power calculation in each sets. (6) Correlate different results until find the correct key conceding that hypothetical key is the real key it can be described by certainly spikes in the different traces or then the key is incorrect.

Since AES have become a FIPS standard in November 2001,various attempts of attack against the AES have been made.By By extensive search,with 256-bit keys,2256 possibilities must be checked,which lead likely impossibility of attacks under such method.

Advanced Encrypyion Standard (AES) is a symmetric encryption algorithm with the motive of being a faster and more secure encryption algorithm over years.The AES cipher is a series of shift which convert the plain text to cipher text by using secret keys.Each round consists of AddRound Key,ShiftRows,MixColumns steps which are linear operations and SubBytes step to be non-linear.

SubBytes step is the first step of AES round.Each byte in the array is updated by a 8-bit substitution box (S-Box),which is derived from the multiplicative inverse over GF (2^8). In the sub bytes operation,S-box is the utmost crictical component,as it regulates the power consumption and throughput of not only the subbytes operation but also the AES hardware implementation.The specific peaks of the DPA trace occur to be closely related to first add round key operation and subbytes operation.AES S-Box is constructed by combining the inverse function with an invertible affine transformation in order to avoid attacks based on mathematics.A block diagram of AES S-Box is shown in fig.1(a).In the consequent MixColumns step,a linear transformation operates on each column of the state,which is two-dimensional array of bytes.The last step,AddRoundKey,it add a round key to the state by doing the bitwise XOR operation in an AES round.

During these years,various counter measures of resisting side-channel analysis attacks have been proposed,including software-based and hardware-based methods.The goal of countermeasures against DPA attacks is to reduce or balance the power consumption.For example,one can insert the random delays,static complementary CMOS logic,or the masked logic.These methods cannot prevent DPA attacks completely because of the power leakage of CMOS circuit.Dual-rail method is the most promising logic style among many countermeasures.Sense Amplified Based Logic (SABL),Wave dynamic differential logic (MDPL) are all based on Dual-rail logic.The aid of dual-rail logic is that the constant power consumption can be achieved since the signals are implemented by two complementary wires.The downside is dual-rail method normally increase the area and time delay.Another good countermeasure is using asynchronous logic,presents that the power dissipated is independent of the input data in asynchronous logic.In this article, we propose an asynchronous AES S-Box based on a Null Conventional Logic (NCL),which matches the two important properties mentioned above;dual-rail encoding and clock-free operation.It is intended to achieve low-power consumption for mobile applications and considerable resistance against side-channel attacks such as DPA

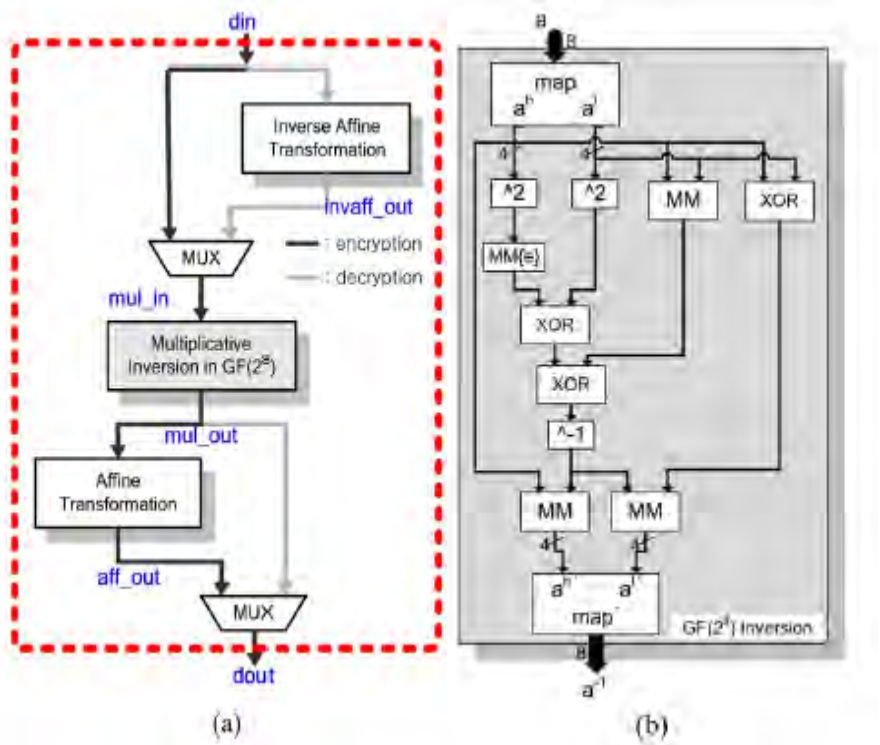

Figure 1: (a) Combinational s-box architecture with encryption and decryption datapaths; (b) Block diagram of multiplicative inversion over GF(2^8) component where MM is modular multiplication and XOR is Exclusive-OR operation.

II. NCL OVERVIEW

NCL is a self-timed logic paradigm in which control is in-herent in each datum.NCL follows the so-called conditions of seitz's delay-insensitive signaling arrangement.Like further delay-insensitive logic methods the NCL paradigm assumes that forks in wires are isochronic.Various aspects of the paradigm,including the NULL logic state from which NCL derives its name,have origins in Muller's work on speed-independent circuits in the 1950's and 1969's.

A. Delay Insensitivity

NCL utilizes symbolic completeness of expression to achieve delay-insensitive behaviour.A symbolically complete expression depends only on the relationships of the symbols present in the expression without reference to their time of evaluation.In particular,dual-rail and quad-rail signals,or further mutually exclusive contention groups can incorporate data and control information into one mixed-signal path to eliminate time reference.

For NCL and other circuits to be delay insensitive,assuming isochronic wire forks,they must meet the input completeness and observability criteria.Completeness of input requires that all the outputs of a combinational circuit may not transition from NULL to DATA until all inputs have transitioned from NULL to DATA,and thet all the outputs of a combinational circuit may not transition from DATA to NULL prior to all inputs have change over from DATA to NULL.In circuits with multiple outputs,it is tolerable.According to Seitz's weak conditions,for some of the outputs to transition without having a complete input set present,since all outputs cannot transition before all inputs arrive.Observability requires that no orphans may propagate through a gate.An orphan is defined as a wire that transitions during the current DATA wavefront,although is not used in the decision of the output.Orphans are generated by wire divaricate and can be neglected through the isochronic fork assumption,As long as they are not allowed to access to cross gate boundary.This observability condition,also referred to as indicatability or stability,ensures that every gate transitions is necessary to transition at least one of the outputs.The observability condition can be relaxed through orphan analysis and still achieve self-timed behaviour;however,this requires some delay analysis.Further more,when circuits use the bit-wise completion strategy with selective input incomplete components,they must also adhere to the completion completeness criterion,which requires that completion signals only be generated such that no two adjacent DATA wavefronts can interact within any combinational component.

Most multirail delay insensitive systems including NCL,have at least two register stages,one at both the input and the output.Two adjacent register stages interact through request and acknowledge lines k and k subsequently,to restrict the current DATA wavefront from overwriting the previous DATA wavefront by ensuring that the two are separated by a NULL wavefront.

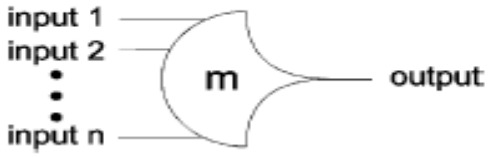

Figure 2 THmn threshold gate.

B.Logic Gates

NCL differs from other delay insensitive paradigms,which use only one type of state holding gate,the c-element.A c-element behaves as follows:when all inputs assume the same value,the output assumes this value;if not,the output does not change.On the other hand,all NCL gates are state holding.NCL utilizes threshold gates as its basic logic elements.The primary type of threshold gate shown in fig .is the THmn gate,where .THmn gates have n single-wire inputs,where atleast m of the n inputs must be asserted before the single-wire output will become asserted. NCL threshold gates are designed with hysteresis state holding capability,such that all asserted inputs must be de-asserted before the output will be deasserted.Hysteresis ensures a complete transition of inputs back to NULL before asserting the output associated with the next wavefront of input data.NCL threshold gates may also include a reset input to initialize their output.Circuit diagrams designate resettable gates by either a D or an N appearing inside the gate,along with gate's threshold.D denotes the gate as being reset to 1,and N to logic 0.The table 1 shows 27 threshold gates and its functions.

III. ASYNCHRONOUS AES S-BOX DESIGN

Asynchronous clockless circuits aims less power,generate less noise and results less electro-magnetic interference compared to their synchronous counterparts.Null Convention Logic (NCL) is a delay-insensitive logic which belongs to the asynchronous circuits categories.NCL circuit utilizes dual-rail and quad-rail logic to achieve this delay in-sensitivity.A dual-rail signal can represent one of available three states,DATA0,DATA1 and NULL,which corresponds to Boolean logic 0 (i.e., DATA0),Boolean logic 1 (i.e., DATA1) and control signal NULL for asynchronous handshaking, respectively.In order to achieve clock free operation,two delay in-sensitive registers on both sides of the combinational NCL circuit with local handshaking signals are needed.In this research,dual-rail signals substitutes for corresponding conventional binary signals in the NCL.

TABLE I
17 FUNDAMENTAL NCL GATES

NCL Gate	Function
TH12	A + B
TH22	AB
TH13	A + B + C
TH23	AB + AC + BC
TH33	ABC
TH23w2	A + BC
TH33w2	AB + AC
TH14	A + B + C + D
TH24	AB + AC + AD + BC + BD + CD
TH34	ABC + ABD + ACD + BCD
TH44	ABCD
TH24w2	A + BC + BD + CD
TH34w2	AB + AC + AD + BCD
TH44w2	ABC + ABD + ACD
TH34w3	A + BCD
TH44w3	AB + AC + AD
TH24w22	A + B + CD
TH34w22	AB + AC + AD + BC + BD
TH44w22	AB + ACD + BCD
TH54w22	ABC + ABD
TH34w32	A + BC + BD
TH54w32	AB + ACD
TH44w322	AB + AC + AD + BC
TH54w322	AB + AC + BCD
THxor0	AB + CD
THand0	AB + BC + AD
TH24comp	AC + BC + AD + BD

The AES S-Box algorithm adapted in this research follows the combinational logic circuit architecture presented in [3].The affine transformation and inverse affine transformation components follow a series of Boolean equations given in table 2.As shown in the table 2,the affine transformation and inverse transformation components requires 16 and 12 XOR gates,correspondingly.

Table 2: Boolean equations for Affine transformation and inverse Affine transformation components.

$q = aff\_trans(i)$	$q = aff\_trans^{-1}(i)$
$i_A = i_0 \oplus i_1, i_B = i_2 \oplus i_3$	$i_A = i_0 \oplus i_5, i_B = i_1 \oplus i_4$
$i_C = i_4 \oplus i_5, i_D = i_6 \oplus i_7$	$i_C = i_2 \oplus i_7, i_D = i_3 \oplus i_6$
$q_0 = \overline{i_0} \oplus i_C \oplus i_D$	$q_0 = \overline{i_5} \oplus i_C$
$q_1 = \overline{i_5} \oplus i_A \oplus i_D$	$q_1 = i_0 \oplus i_D$
$q_2 = i_2 \oplus i_A \oplus i_D$	$q_2 = \overline{i_7} \oplus i_B$
$q_3 = i_7 \oplus i_A \oplus i_B$	$q_3 = i_2 \oplus i_A$
$q_4 = i_4 \oplus i_A \oplus i_B$	$q_4 = i_1 \oplus i_D$
$q_5 = \overline{i_1} \oplus i_B \oplus i_C$	$q_5 = i_4 \oplus i_C$
$q_6 = \overline{i_6} \oplus i_B \oplus i_C$	$q_6 = i_3 \oplus i_A$
$q_7 = i_3 \oplus i_C \oplus i_D$	$q_7 = i_6 \oplus i_B$

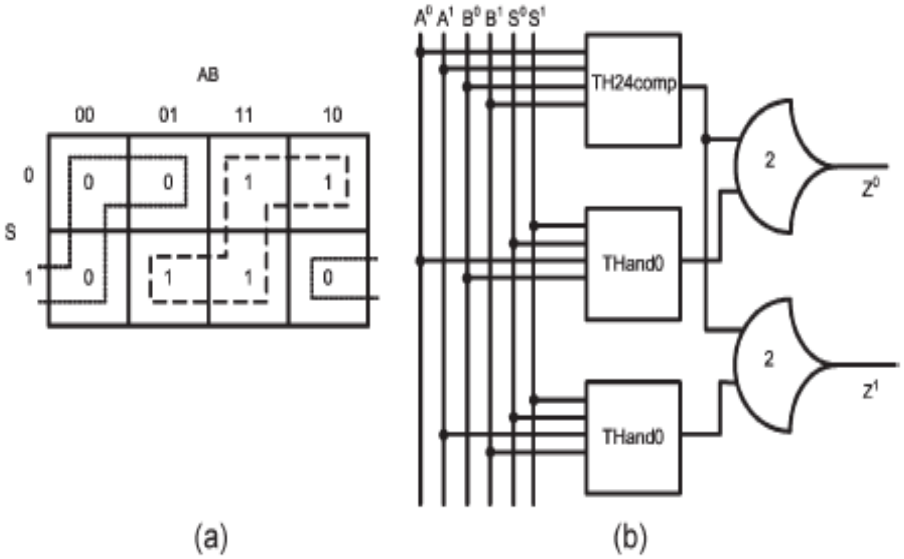

Figure 3: (a) K-map for NCL Multiplexer; (b) Optimized NCL Multiplexer.

The multiplicative inversion in GF(2^8) follows the procedure shown in Fig 1(b).Map,square,multiplication operations also require significant amount of XOR gates of which the sum is 95.To convert the conventional S-Box into NCL,replacing the Boolean XOR and AND operation into a dual-rail NCL gate is required.

Besides a series of XOR gates with AND gates,two NCL multiplexers are needed for switching between encryption and decryption process.Unlike Boolean logic,NCL has 27 fundamental threshold gates to realize arbitrary logic.In order to achieve the input-completeness and observability,it is important to choose appropriate threshold gates.For example,in the design of a 2:1 multiplexer,according to the Karnaugh map in fig 3(a),the sum-of-product (SOP) functions can be simplified as follows,

$$Z^0 = A^0 S^0 + S^1 B^0;$$

$$Z^1 = A^1 S^0 + S^1 B^1;$$

After modifying both functions for input-completeness, new SOP functions are obtained as follows,

$$Z^0 = A^0 S^0 (A^0 + A^1)(B^0 + B^1) + S^1 B^0 (A^0 + A^1)(B^0 + B^1);$$

$$Z^1 = A^1 S^0 (A^0 + A^1)(B^0 + B^1) + S^1 B^1 (A^0 + A^1)(B^0 + B^1);$$

Both of them can be mapped to a NCL circuit with a TH24comp gate, a THand0 gate and a TH22 gate.The finalized NCL MUX logic diagram is shown in Fig 3(b).

Additionally,XOR function and AND function can also be implemented by threshold gates.An input-complete XOR logic is mapped to two TH24comp gates.An input-complete AND logic is mapped to a THand0 and a TH22 gate.The finalized NCL XOR and AND logic diagrams are as shown in Fig 5.

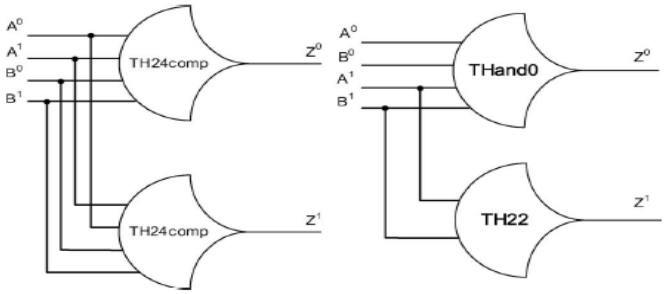

Figure 5: (Left) Input-complete NCL XOR and (right) NCL AND function for the proposed NCL S-Box.

IV. FUNCTIONAL VERIFICATION OF THE PROPOSED NCL S-BOX DESIGN

VHDL is used as a Hardware Description Language because of its flexibility to exchange among environments.The proposed NCL S-Box has been implemented in VHDL and simulated with ModelSim by Mentor Graphics. In order to conceive more tricky operation,LFSR (Linear Feedback Shift Register) is used as a countermeasure circuit. .LFSR is a shift register,when clocked,advances the signal through the register from one bit to the next most significant bit.It is a special type of counter which has its counting sequence of about pseudo random.The plain text is given as input to the LFSR. The output of LFSR delivers its output to the Asynchronous S-Box as its input,to make it not easy to predict the count series.The outcome product of asynchronous S-Box is analysed and is shown as waveform in Fig 6.

By referring the waveform shown on Fig 6,the initial value of the input and output is NULL and DATA0,respectively, as previously input register is reset to NULL and output register is reset to DATA.As soon as reset falls down to 0,k_o from the output register becomes 1 and k_o for the input register connected to k_o turn to 1.Just as k_i rises,the input is changed to the waiting input signal,0101010101010110 in dual-rail signaling which means 00000001 in Binary.Due to the propagation delay, the output arrives in approximately 5ns to be 0110101010100101 in NCL which means 01111100 in Binary.As every bit of the output signal changes to either DATA0 or DATA1 from NULL, k_o falls to 0 which means the output register has received the proper output DATA wave.

Table 3 shows the encryption and decryption simulation results for 10 arbitrary sample inputs,5 for encryption and 5 for decryption,correspondingly.On the NCL S-Box output column,the outcomes are displayed as 16 bits,which are the drag out dual-rail signals.For example,for input 122,the NCL S-Box output is 10 01 10 10 01 10 10 01 in Binary which matches to the output of the synchronous S-Box.

Table 3: Simulation results for 20 arbitrary samples from conventional synchronous S-Box and the proposed NCL S-Box.

Simulation Results			
Mode	Input	Output	
		S-Box	NCL S-Box
Encrypt	9	00000001	0101010101010110
	26	10100010	1001100101011001
	106	00000010	0101010101011001
	122	11011010	1001101001101001
	158	00001011	0101010110011010
Decrypt	32	01010100	0110011001100101
	51	01100110	0110100101101001
	156	00011100	0101011010100101
	185	11011011	1010011010011010
	203	01011001	0110011010010110

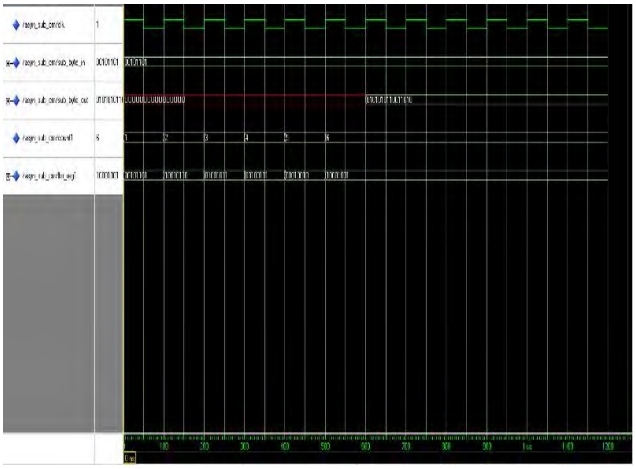

Figure 6: Mentor Graphics ModelSim waveform for the proposed NCL S-Box

V. POWER CONSUMPTION SIMULATION AND COMPARISON

After the functional verification,the VHDL code has been synthesized and its power measurements are executed using XILINX ISE simulator.Power simulation results from XILINX ISE simulator for the proposed NCL S-Box and conventional synchronous S-Box are shown in Fig 7.As Fig 7 shows the proposed NCL S-Box has 165 mW and conventional synchronous S-Box has 174 mW for Temperature about 27 degree Celsius.

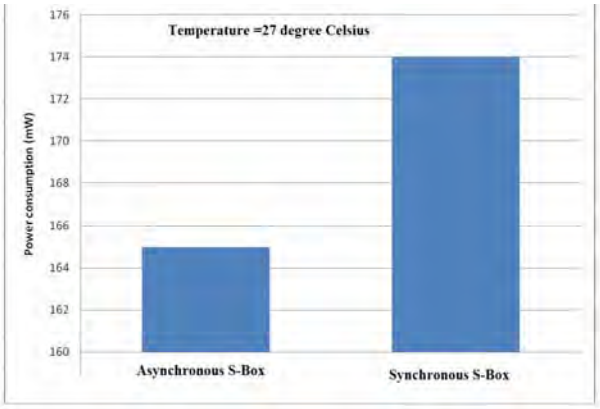

Figure 7: Total estimated power consumption.

VI. CONCLUSION

A new asynchronous combinational S-Box design for AES cryptosystems has been proposed and validated in this work.The proposed S-Box design is based on a delay-insensitive logic paradigm known as Null Convention Logic (NCL) and achieves improved low power operation and DPA-resistance over its clocked counterpart.The proposed NCL AES S-Box has been implemented in VHDL and simulated with Mentor Graphics EDA tool set.Various tools including ModelSim,Accusim,Design Architect-IC,Eldo and AdvanceMS have been used to perform functional verification,low–power operation and DPA-resistance.The proposed design has been compared with the existing synchronous combinational logic AES S-Box design and both reduced power consumption and improved DPA-resistance has been verified.

REFERENCES

[1] J. Kocher, P. Jaffe, and B. Jun, “Introduction to differential power analysis and related attacks,” Cryptography Res. Inc., San Francisco, CA, 1998,Tech. Rep.
[2] J.-S. Coron, “Resistance against differential power analysis for,Elliptic Curve cryptosystems,” in Proc. 1st Int. Workshop CHES, 1999, pp. 292–302.
[3] W.Johannes, O. Elisabeth and L.Mario,”An ASIC Implementation Of the AES SBoxes”,Topics in cryptology,CT-RSA 2002,LNCS,Vol. 2271 ,pp.29-52, Jan 2002.
[4] K. Tiri and I. Verbauwhede, “Securing encryption algorithms against DPA at the logic level: Next generation smart card technology,” in Proc.Workshop CHES, 2003, pp. 125–136.
[5] D. Sokolov, J. P. Murphy, A. Bystrov, and A. Yakovlev, “Improving the security of dual-rail circuits,” in Proc. Workshop CHES, 2004,pp. 282–297.
[6] P. Kocher, “Design and validation strategies for obtaining assurance in countermeasures to power analysis and related attacks,” in Proc. NIST Phys. Security Workshop, 2005, pp. 1–11.
[7] L. Angrisani, M. D’Apuzzo, and M. Vadursi, “Power measurement in digital wireless communication systems through parametric spectral estimation,”IEEE Trans. Instrum. Meas., vol. 55, no. 4, pp. 1051–1058,Aug. 2006.
[8] D. Macii and D. Petri, “Accurate software-related average current drain measurements in embedded systems,” IEEE Trans. Instrum. Meas.,vol. 56, no. 3, pp. 723–730, Jun. 2007.
[9] Y. Han, X. Zou, Z. Liu, and Y. Chen, “Improved differential power analysis attacks on AES hardware implementations,” in Proc. Int. Conf.Wireless Commun., Netw. Mobile Comput., Sep. 2007, pp. 2230–2233.
[10] J. Hunsinger and B. Serio, “FPGA implementation of a digital sequential phase-shift stroboscope for in-plane vibration measurements with subpixel accuracy,” IEEE Trans. Instrum. Meas., vol. 57, no. 9, pp. 2005–2011, Sep. 2008.
[11] A. Bogdanov, “Multiple-differential side-channel collision attacks on AES,” in Proc. CHES, 2008, pp. 30–44.
[12] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, “Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits,”IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57, no. 2, pp. 355–367,Feb. 2010.
[13] M. Lazzaroni, V. Piuri, and C. Maziero, “Computer security aspects in industrial instrumentation and measurements,” in Proc. IEEE I2MTC,May 2010, pp. 1216–1221.
[14] R. Jevtic and C. Carreras, “Power measurement methodology for FPGA devices,” IEEE Trans. Instrum. Meas., vol. 60, no. 1, pp. 237–247,Jan. 2011.
[15] J. Wu, Y. Shi, and M. Choi, “FPGA-based measurement and evaluation of power analysis attack resistant asynchronous s-box,” in Proc. IEEE I2MTC, May 2011, pp. 1–6.