

# DPA on Faulty Cryptographic Hardware and Countermeasures

Konrad J. Kulikowski, Mark G. Karpovsky, and Alexander Taubin

Reliable Computing Laboratory, Boston University  
8 Saint Mary's Street, Boston, MA 02215  
{konkul, markkar, taubin}@bu.edu

**Abstract.** Balanced gates are an effective countermeasure against power analysis attacks only if they can be guaranteed to maintain their power balance. Traditional testing and reliability methods are used primarily only to ensure the correctness of the logical functionality and not the balance of a circuit. Due to the hardware redundancy in balanced gate designs, there are many faults which can imbalance a balanced gate without causing logical errors. As a result, traditional testing and reliability methods and architectures are unable to test and verify if a gate is completely defect and fault-free and hence balanced. Our simulations show that a few faulty balanced gates can make a circuit as vulnerable to power analysis attacks as a completely imbalanced implementation. This vulnerability opens the possibility of new methods of attacks based on a combination of fault and power attacks. A solution to the vulnerability based on a built-in differential self-balance comparator is presented.

## 1 Introduction

Cryptographic algorithms are vulnerable to attacks which exploit the physical characteristics of their hardware implementations. The formal security models of cryptographic algorithms assume that information about the intermediate data during computation (encryption, decryption, etc.) is not available to an adversary. An adversary with access to intermediate data can drastically decrease the complexity of cryptanalysis. Examining the power consumption or behavior in the presence of faults of a device can provide such information to an attacker. Efficient methods for performing power analysis and fault analysis attacks have been developed which can analyze the side-channels and extract useful information which can be used to aid in cryptanalysis.

To prevent such attacks several countermeasures have been proposed which aim to reduce or eliminate the amount of information which can be inferred about intermediate data in a hardware implementation of a cryptographic algorithm. Traditionally, the power and fault attacks and their countermeasures have been considered and developed separately. One of the most effective countermeasures against power analysis attacks is based on the use of specially designed balanced gates for which the power consumption is equal for all data and all transitions of the gate. Several such gates have been previously presented (SABL [1], DyCML [2], BSDT [3], WDDL [4], Replication Gates [5]). The proposed fault attack countermeasures have been based on adding redundancy to the device, usually in the form of error-detecting codes, to detect errors in the logical values of the processed data (i.e. [6-8]).

Balanced gates and error-detecting codes are effective countermeasures for their respective attacks if the side-channels are considered separately. The details of the proposed countermeasures and a joint consideration of both power and fault side-channels raises several practical security limitations of the approaches. There are several major limitations and potential problems with the current power and fault countermeasures which stem from the redundancy associated with balanced gate designs when power and fault attacks are considered together.

All the currently known balanced gate designs require considerable hardware redundancy and overhead to ensure balanced computations (2.5 to 10x area overhead over standard synchronous static-CMOS implementations). Much of this redundant hardware is not directly associated with the logical or Boolean function of the gate; it is present to ensure power balance during computations. The additional consideration of data independent power consumption means that a gate's primary functionality is no longer limited just to its logical or Boolean function. The power balance of the gate is just as important. Weaknesses in the present balanced gate designs exist due to the redundancy of the gate; there exist many internal transistor level faults which will not affect the Boolean function of the gate but will affect the balance of the gate.

There are a number of methods to ensure proper Boolean functionality of circuits in all stages of the device's lifecycle. Techniques for post manufacturing testing, built in self-test (BIST), and on-line testing have been developed and are available for a variety of applications. While the methods which ensure proper Boolean functionality and hence provide reasonable protections against traditional fault attacks are mature, there are practically no developed architectures, methods, or techniques for testing and verification of the other crucial component of a gate's functionality: its balance.

The inability to ensure proper balance functionality during the lifecycle of a device creates a serious security weakness. The security of the cryptographic devices is dependent on the balance of the circuit. Without methods to test or verify this balance no guarantees can be made about the security. Moreover, the lack of built-in self balance test (BISBT) opens a possibility of combined fault and power attacks. The addition of a few imbalances, either from natural effects or from malicious tampering, can make it possible to perform established power analysis attacks even on protected devices.

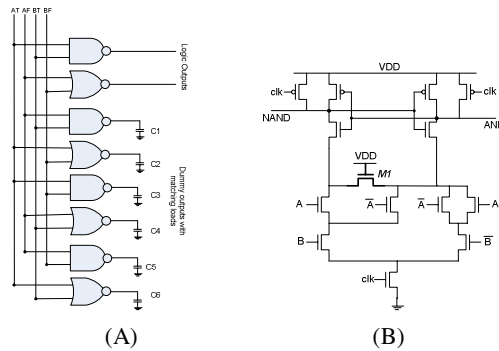
The next section analyzes some proposed balanced gate designs and shows that faults can easily be manifested in a circuit which can imbalance the proposed gates without changing the gate's functionality. The effects of a few imbalances in a circuit are analyzed. The proposed countermeasures and research avenues for developing BISBT techniques and architectures are examined.

## 2 Vulnerabilities of Existing Balanced Gates

The additional constraint of data independent power consumption translates to more complex and more elaborate gate designs than the traditional minimal static CMOS gate implementations. The additional structures necessary to meet the balance requirements create redundancy with respect to the structures which are necessary for the Boolean functionality. Indeed, all current balanced gate designs are based on dual-rail return-to-zero (RTZ) signaling protocols which have an inherent hardware

overhead. The two respective functions of a balanced gate are mostly separate and correct operation of one of the functionalities does not imply the correctness of the other functionality.

Examples of two balanced gates styles which demonstrate this redundancy and partial separation of functionalities are pictured in Figure 1. The two gate styles represent the two ends of a spectrum of the approaches to balanced gate design. The first, (Figure 1A) proposed by Jaffe et al. in [5], balances gates with the use of standard unsecured static CMOS gates to create a larger balanced gate. Approaches such as this one have very large overheads but also have an advantage in that existing standard-cell libraries can be used reducing the development costs. The other end of the spectrum is exemplified with the SABL gate, (Figure 1B) proposed by Kris Tiri et al. in [1]. The SABL gate is a much more compact, highly specialized implementation but requires a custom dedicated standard-cell library or a completely custom design flow. Both of these implementations have redundancy which is not directly associated with the Boolean functionality of the gate.



**Fig. 1.** (A). Balanced NAND gate proposed by Cryptographic Research (B). SABL AND-NAND gate with enhanced special DPDN

The first balanced gate design, shown in Figure 1A, requires a 700% hardware redundancy to achieve balance. The gate combines a dual-rail design with additional gates which are used to balance the internal switching characteristics of the sub-gates. In the resulting balanced gate the bottom 6 sub-gates of the larger balanced gate shown in Figure 1A are only used for balancing purposes and are not connected to logical outputs of the gate. The SABL gate, Figure 1B, has a similar, but smaller, redundancy. Specifically, transistor's M1 function is to discharge all the internal capacitance of the whole gate for every cycle of operation and has no direct Boolean purpose.

If the implementations can be guaranteed to be 100% reliable, then this hardware redundancy in itself is not a problem. The complications with such arrangements arise when the reality of physical devices, the imperfect manufacturing methods, and the adaptability of an active attacker are considered.

The fact that real devices are not perfect and not completely reliable has been a crucial consideration in standard circuit and system level design. Through the years a

vast number of techniques and architectures have been developed to test and verify a device's functionality throughout its complete life-cycle. Methods for testing and verification for on-line and post manufacture are all indispensable to today's digital devices to ensure reliability and correct operation. Testing and fault hardening is of even more importance where the correct functionality of the device is crucial to the safety or security of a system. However, virtually all of the developed testing and reliability methods have been based around ensuring and verifying the correct functionality of the Boolean function of the device. Testing and reliability measures for the power functionality, in terms of power balance, have not been previously considered and there are neither developed methods nor architectures for ensuring balanced computations. Manufacturing a component for a critical application without verification and built-in reliability measures is unthinkable for standard Boolean circuits considering process yields and reliability of devices which are only declining as a result of scaling.

Aside from performing a full differential power analysis (DPA) attacks or other statistical analysis [9] on a manufactured circuit there have been no known methods for balance verification since the actual differences in current and behavior of a balanced circuit and an imbalanced faulty circuit are almost indistinguishable by normal current testing techniques such as IDDQ [10] and IDDT [11]. Verification by performing an attack for all parts of the designed circuit is impractical due to the dramatic increase in time and hence the cost of the procedure. Even if the drastic cost increase can be acceptable for some applications there are still no methods or mechanisms to ensure proper balanced functionality once the device is deployed.

Relying only on Boolean testing and reliability measures to detect defects and faults is not adequate. In existing designs there is not a complete overlap between the structures necessary for the balanced-power and Boolean functionality of a gate. As a result there are faults and failures (transistor failures, open circuits, wire shorts, etc) which can easily imbalance the gate without affecting the Boolean functionality. This non-overlapping functionality can be drastic as in, for example, the gate in Figure 1A where over 75% of the hardware of the gate is used only for balancing purposes. For that implementation it means that a fault is over three times more likely to affect the balance functionality than the Boolean functionality of the gate. About 75% of faults would not be detected if only the traditional Boolean off-line testing and on-line self-error- detecting methods based on error-detecting codes are used. A similar effect is also present in the SABL gate style shown in Figure 1B. Although the percentage of faults which can imbalance but not affect the logical function of the gate is smaller it is still not comparable to the reliability measures for key life-time requirements for cryptographic algorithms which are on the order of  $2^{-40}$  [12].

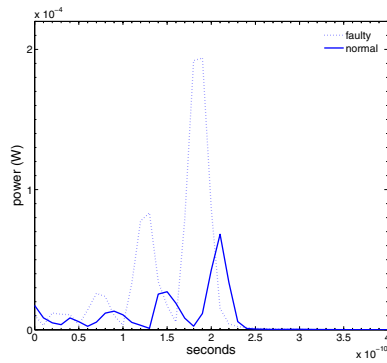
Even with the optimized gates such as the SABL gate, there is still the need for additional methods and considerations which will ensure balance at a comparable level to that of the logical functionality. The problem of weakened security due to undetectable failures is a real threat. Without a guaranteed level of balance no precise estimates can be given about the security of the device (in terms of power analysis attack resistance). A couple of faults can easily imbalance a circuit making power analysis attacks easier than the original design seemed to ensure.

The next section will show an example of the realistic nature of such weaknesses in the balanced SABL gate implementations.

### 3 Effects of Failures on Imbalance and Power Analysis Attacks

To demonstrate the effects of faults on balanced gates and their consequence on power analysis attacks faulty versions of the SABL style gates were simulated. The resulting imbalances were measured and compared to the non-faulty gates. To illustrate how a few imbalance-causing faults can affect a DPA attack was simulated on a substitution box (Sbox) of the Data Encryption Standard (DES) implemented with both normal and faulty SABL [1] gates.

The SABL gate represents the state-of-art for synchronous balanced gate designs. It is a compact and optimized dynamic implementation which has a high level of balance and small level of redundancy. Despite the optimized design the gates still have areas of redundancy which are only used for balancing purposes. Using a simple fault model, the gate can easily be imbalanced without affecting the logical output of the gate.



**Fig. 2.** Absolute power imbalance of a correctly functioning and a faulty SABL AND/NAND gate during the evaluation phase

For the properly functioning SABL AND/NAND gate implemented in a 0.18 $\mu$ m technology assuming equal output load capacitances on both data output rails there is relatively little temporal difference in the gate's power signature. Figure 2 shows the absolute imbalance of the gate with respect to time where the magnitude of the curve represents the value of the instantaneous power consumption for the four possible input combinations.

To imbalance the gate pictured in Figure 1B, the gate VDD voltage of the M1 transistor was removed simulating a simple open circuit fault. As a consequence of the disabled transistor the effective internal balance of the gate is reduced to that of a normal differential dynamic gate. By disabling the M1 transistor, practically all the benefits of using a sense-amplified balanced design are removed. The effective absolute power imbalance of the gate is effectively more than doubled. The injected fault has no effect on the logical output of the gate. The gate continues functioning correctly in all respects except its balance. Many other more drastic faults can be envisioned which could create larger power imbalances.

Full analog SPICE simulations were performed on a Sbox of DES to evaluate the impact a small number of faulty gates can have on power analysis attacks. The circuit is a small component of a complete symmetric cryptosystem. The Sbox is usually the circuit component which is targeted for power analysis attacks. The simulation circuit, shown in Figure 3, is composed of 137 two-input OR, AND, and XOR gates. It has a 10-bit text input, a 6-bit secret-key input and a 4-bit output. The Sbox1 combinational circuit was automatically synthesized from a table specification using Design Compiler from Synopsys. The circuit was simulated on the transistor level (schematic level, pre layout) using the analog Spectre simulator from Cadence for all of the 1024 input combinations and fixed key input. The power consumption of the circuit was recorded and then analyzed by performing a Differential Power Analysis attack.

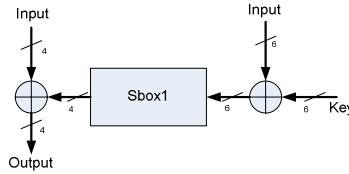


Fig. 3. Circuit used for DPA simulations

The DPA attack was performed by finding the measured power and hypothesis correlation on the 4-bit output of the Sbox by using the Pearson's correlation coefficient  $C(M, P)$ :

$$C(M, P) = \frac{\mu(M, P) - \mu(M)\mu(P)}{\sqrt{\sigma^2(M)\sigma^2(P)}} \tag{1}$$

where  $P$  is the set of predictions,  $M$  is the set of recorded power measurements,  $\mu(X)$  is the mean of the set  $X$  and  $\sigma^2(X)$  is its variance. The Pearson's correlation coefficient gives a measure of the data dependence of the power consumption. A survey of correlation methods and attacks on S-boxes can be found in [13].

In comparing the security of vulnerability of balanced gate designs the most common method has been to determine the number of necessary power measurements for disclosure of the secret key. Since the simulations performed are only on a small circuit with a very limited number of inputs and no additional circuitry which would create noise and etc. we used a new comparison approach.

An important practical aspect in considering the feasibility of a power attack is to evaluate the required capability of an attacker which is necessary for a successful attack. An important capability consideration is the required sophistication of the measuring equipment or rather the required minimal precision for estimation of a power consumption which is necessary to have a successful attack. The necessary precision was used as a comparison metric. All simulations and all the data were recorded with the maximum level of precision of the simulator. After all the power data was recorded the precision of the measurements was incrementally reduced until the attack was no longer successful. The reduction of precision was based the following formula:

$$rp = np - np \text{ mod}(precision) + precision * rand() \quad (2)$$

where  $rp$  are the reduced precision measurement,  $np$  are normal precision measurements,  $precision$  is the maximum assumed precision capability of the attacker, and  $rand()$  is a random number from the interval  $[-1,1]$ .

**Table 1.** Minimum required measurement precision for a successful DPA attack for normal and faulty implementations of the DES Sbox

Implementation	Min required measurement precision for successful DPA
Normal	$5.5 \times 10^{-4} W$
Four Gates Faulty	$11.2 \times 10^{-4} W$
All Gates Faulty	$11.6 \times 10^{-4} W$

The consequences on the required precision of the measurements for all input combinations for the normal and faulty Sbox test circuits are shown in Table 1. The results shown in Table 1 provide for a relative comparison of the results of faults within the circuit. It should be noted that the absolute precision values might not completely reflect the precision required for an actual physical attack on a complete circuit. The simulation results are based on ideal measurements from a small test circuit. Actual attacks and measurements would be subject to noise of additional power consumption of the extra circuitry, timing uncertainty in measurements, as well as additional capacitive and inductive effects from packaging and probing materials. These effects would certainly reduce the capacity to perform successful attacks. In physical attacks it should be expected that the absolute values of the minimum precision required should be lower (more precision would be required) than the table suggests. However, the relative value of the minimum precision should still be accurate and provide for an accurate relative comparison of the effects of faults on power analysis.

The first row in Table 1 represents results from simulations performed on the normal non-faulty SABL implementation. This value is used as a relative reference point for comparison. The absolute minimum precision measurement value required for successful DPA analysis was slightly more than four times the imbalance of a normal SABL AND gate (Figure 2). This absolute value of the necessary precision reflects the fact that four Sbox outputs were targeted for the attack and hence it was their driving gates whose combined imbalance was observed in Table 1. For the second result in Table 1, the four output gates of the 137 2-input gates which make up the Sbox were made faulty by making the gate terminal of the M1 transistor disconnect from VDD. The effective imbalance of the faulty gates was doubled as shown in Figure 2. Although only a small fraction of the gates were imbalanced, the necessary minimum precision necessary for a successful attack more than doubled. The minimum precision required for the attack increased proportionately to effective imbalance of the individual gate. Moreover as the last row of Table 1 indicates, the effect of just a few imbalanced gates on the required precision of DPA was almost equal to that

of the implementation in which all the gates are faulty. The implementation in which all the gates were faulty is roughly equivalent to an unprotected normal implementation based on differential dynamic logic.

The above results demonstrate the criticality of considering faults on balanced gates. As the results suggest, only a few imbalanced gates are enough to make a protected implementation be as vulnerable to DPA analysis as an unprotected implementation. In compact implementations, for example in some sensor network applications, the datapath widths are kept at a minimum to meet the required maximum instantaneous power requirements. In such implementations where the datapath can be as small as 8 bits, a single fault which causes an imbalance can be enough to reveal a complete key and completely compromise the security of the device.

## 4 Countermeasure Strategies

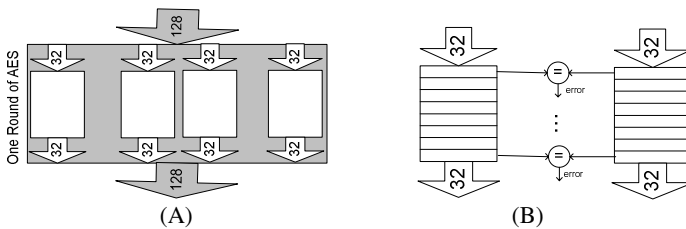
The experimental results from the previous section confirm that the inability to verify and check balanced computation can create serious holes in the security of even “protected” cryptographic devices. Architectures and methods for detecting imbalance need development. Detection of imbalances is a difficult paradigm shift in that it requires an exact consideration of an analog continuous functionality, the power consumption of the device, in hardware which is optimized for digital processing. Some possible countermeasures are considered next.

One of the least invasive methods to combat the problem would be to redesign the balanced gates so that all internal faults which can cause imbalances will also cause logical faults. This would allow the use of existing error detection architectures and techniques which are already a standard requirement on secured hardware for the prevention of fault analysis attacks. If successful, this approach would greatly simplify the additional design tasks since after one redesign, everything else would involve “standard” considerations. However, due to the large difference between Boolean and balance functionalities the chances of success of this approach are small as exemplified in the designs of current balanced gates which are unable to meet this requirement.

Another possible approach is to adapt existing analog based techniques used in testing. In architectures based on IDDQ and IDDT Built-in Self Test approaches the circuit is tested by measuring its current or power consumption while it performs predetermined computations. The current is then compared with a stored reference value. Any differences (exceeding a selected threshold) from the predetermined signature can mean faults within the circuit. One disadvantage of this approach is the inherent complexity of performing comparisons with a stored reference value. To detect imbalances the built in test circuits needs to record, digitize and compare the power signatures to a stored reference value (threshold for current consumption) with a high level of accuracy. The necessary precision translates into large and precise Analog to Digital (AD) converters which require substantial amount of hardware. Thus the approach is only suitable for larger designs where one current sensor is used for a large portion of the circuit. Even more problematic is the fact that since the current and power consumptions of circuits vary depending on temperature, process variability and voltage levels the thresholds used for comparing good and bad circuits needs to

be quite lax. As a result mostly catastrophic or short circuit faults in the original and redundant parts of the device can be tested in this manner and the sensitivity needed to determine if some gates are only out of balance is beyond the capabilities of the method.

A possible solution to the problem which overcomes the drawbacks of the previously mentioned approaches is based on modifying some of the concepts present in IDDQ testing. The solution also exploits the symmetry which is present in many cryptographic hardware implementations. The approach is based on a number of distributed analog voltage or current comparators whose detection capability can be propagated into a conventional digital alarm signal (which can be used to disable the device). The details of this approach, which will be referred to as a built-in differential self balance test (BISBT), are discussed in the remainder of this section.



**Fig. 4.** (A) Datapath of one Round of AES is divided into four separate parallel slices. (B) Sub-division of parallel slices with an analog comparator to check for equal power consumption.

Many of the encryption algorithms, especially symmetric key algorithms such as the Advanced Encryption Standard (AES) [14], have lots of symmetry in their structure. In AES-128 (AES with a 128 bit key) for example, the 128 bit parallel datapath of each round of the algorithm is divided into four 32-bit independent and parallel slices each of which is composed of exactly the same hardware (Figure 4). (These parallel slices are also internally divided into smaller parallel slices.) The data along the complete 128-bit datapath is generally synchronized and all slices perform the exact same functions but on different data. If the circuits of the slices are implemented with truly balanced gates which are functioning correctly then the power consumption of all the respective slices should be practically equal even if the circuits are processing different data. **More importantly, the power consumption of the two circuits which are processing different data will be the same only if their implementations are balanced.**

The proposed differential balanced comparison approach exploits the above mentioned property of balanced design by partitioning the parallel slices of the data path so that a small analog comparator can be used to compare the current consumption of two equal circuit components from respective slices (Figure 4b). The comparator should have a suitable maximum difference threshold upon which a latch in the comparator is set to indicate an imbalanced operation. This error signal can be, in the case of asynchronous fine-grained balanced gate implementations [15, 16], used to stall the pipeline thereby providing a distributed protection mechanism without a single point of failure.

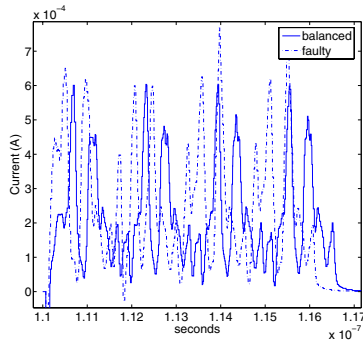
This approach allows a distributed protection because the balance check is not based on an absolute stored reference value but on a low cost comparison. The comparison operation generally requires much smaller hardware since neither AD converters nor memory is needed. Additionally, since the method is based on a comparison of power of two equal circuits which are on the same chip the method is not sensitive to temperature and manufacturing variability which is a large problem with reusing normal IDDQ or IDDT testing methods. Both of the compared circuits will be subjected to the same temperature fluctuations. Likewise, because the small circuits can be grouped locally within a chip, they will be subject only to the local manufacturing process variability effects. Finally, one of additional benefits is that such protection is that it is continuously active whenever the module operates; there would be no need for a special test cycle.

The critical requirement of this method is best possible balance of gates. The balance of the gates will determine the maximum size of the comparison circuits, the maximum granularity, and the required sensitivity of the comparator. As a first order evaluation of the critical parameters of the comparator the power effect details of faults was examined for the balanced symmetric with discharge tree (BSDT) gates [3].

For the initial feasibility experiment two AND gates were simulated side by side with identical inputs and timing. In one of the gates stuck-at faults were injected. The current used by each gate was recorded and compared. Of special interest were those faults which were logically undetectable but could potentially imbalance a gate. An exhaustive set of stuck at faults was injected into one of the gates. The gates were simulated for all possible input combinations. Example current comparison curves of normal and faulty gates for two logically undetectable faults are shown in Figure 5. All of the injected faults produces large differences in the temporal power signatures which are easily identifiable by a current comparison. The internal undetectable faults in the functional block produced large differences in the current consumption of the AND gates. Most faults resulted in a shift and amplitude difference of the current curves which are easily recognizable in the power. The current differences needed to be observed by a comparator are on the order of  $5 \times 10^{-4} A$ , which is two orders of magnitude larger than the normal imbalance of a gate. As was shown in [3] the maximum temporal current difference of a balanced BSDT-style AND gate was no more than  $6 \times 10^{-6} A$  in post layout simulations.

Additionally, the power fault simulations show that this method can also serve as a natural compliment to traditional built-in reliability measures since it is able to detect many faults or errors which cause logical errors. For example, faults which created an invalid value on the dual-rail output of the BSDT gate (11) also resulted in large temporal current differences which can be detected by a comparator.

Based on the initial experiments, it should be practical to place a differential current comparator for partitions of 50 to 60 gates. If a comparator can be on the order of 40 transistors then the overhead will be lower than a traditional BIST architecture. Many of the physical design components, such as current sensors and differential amplifiers, have been developed for IDDQ BIST architectures and can potentially be adapted for this application but many challenges remain in fine tuning the methods to achieve the necessary sensitivity and speed.



**Fig. 5.** The effect of a logically undetectable fault in the functional block on power where dotted and solid lines are for the faulty and normal AND gate respectively

## 5 Conclusions

As the approaches and architectures for balanced gate designs mature many practical considerations need to be addressed. Reliability and balance preserving fault tolerance will be of critical importance. As it has been shown in this paper, a small number of faults can potentially make power analysis attacks feasible even on protected devices. Due to the redundancy of balanced gates these faults might not create logical errors and hence would not be detected by traditional voltage level testing and reliability measures. A possible solution method was described which exploits the symmetry of cryptographic hardware and the operation of balanced gates.

## Acknowledgements

This work was partially supported by a grant from OmniBase Logic Inc.

## References

1. Tiri, K., M. Akmal, and I. Verbauwhede. A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards. 28th European Solid-State Circuits Conference (ESSCIRC 2002), pp. 403-406, September 2002
2. Mace, F., F. X. Standaert, J.J. Quisquater, J.D. Legat, A Design Methodology for Secured ICs Using Dynamic Current Mode Logic, Lecture Notes in Computer Science, Volume 3728, Aug 2005, Pages 550 - 560
3. MacDonald, D.J., A Balanced-Power Domino-Style Standard Cell Library for Fine-Grain Asynchronous Pipelined Design to Resist Differential Power Analysis Attacks. Master of Science Thesis. 2005, Boston University: Boston, available at [http://reliable.bu.edu/Projects/MacDonald\\_thesis.pdf](http://reliable.bu.edu/Projects/MacDonald_thesis.pdf).
4. Tiri, K. and I. Verbauwhede, A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. Design, Automation and Test in Europe Conference (DATE 2004), pp. 246-251, February 2004.

5. Jaffe, J., P. Kocher, and B. Jun, "Hardware-level mitigation and DPA countermeasures for cryptographic devices" US Patent 6654884.
6. Karpovsky, M., K. Kulikowski, and A. Taubin. Differential Fault Analysis Attack Resistant Architectures for the Advanced Encryption Standard. in Proc. World Computing Congress, CARDIS, pp. 177-192, 2004.
7. Kulikowski, K., M. Karpovsky, and A. Taubin. Robust Codes for Fault Attack Resistant Cryptographic Hardware. in Fault Diagnosis and Tolerance in Cryptography, 2nd International Workshop. 2005. Edinburgh.
8. Karri, R., G. Kuznetsov, and M. Gossel. Parity-Based Concurrent Error Detection of Substitution-Permutation Network Block Ciphers. Lecture Notes in Computer Science, Volume 2779, Sep 2003, Pages 113 - 124
9. Coron, J.S., D. Naccache, and P. Kocher, Statistics and Secret Leakage. Trans. on Embedded Computing Sys. 3, 3 (Aug. 2004), 492-508.
10. Rajsuman, R., Iddq testing for CMOS VLSI. Proceedings of the IEEE, 2000. 88(4): p. 544-568.
11. Su, S.-T., R.Z. Makki, and T. Nagle, Transient power supply current monitoring - A new test method for CMOS VLSI circuits. Journal of Electronic Testing, 1995. 6(1): p. 23-43.
12. Gregorio, A.D. Cryptographic Key Reliable Lifetimes: Bounding the Risk of Key Exposure in the Presence of Faults. in FTDC. 2005.
13. Canovas, C. and J. Clediere, What do S-boxes Say in Differential Side Channel Attacks?, in IACR e-Print archive. 2005/311.
14. FIPS PUB 197: Advanced Encryption Standard, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
15. Smirnov, A., A. Taubin, and M. Karpovsky. An Automated Fine-Grain Pipelining Using Domino Style Asynchronous Library. in ACSD 2005: Fifth International Conference on Application of Concurrency to System Design. 2005.
16. Kulikowski, K., A. Smirnov, and A. Taubin. Automated Design of Cryptographic Devices Resistant to Multiple Side-Channel Attacks. in Cryptographic Hardware and Embedded Systems (CHES), 2006.