Asynchronous Balanced Gates Tolerant to Interconnect Variability

Konrad J. Kulikowski, Vyas Venkataraman, Zhen Wang, Alexander Taubin, Mark Karpovsky
Reliable Computing Laboratory
Boston University
Boston, MA 02215
Email: {konkul,vyas,lark,taubin,markkar}@bu.edu

***Abstract*— Existing methods of gate level power attack countermeasures depend on exact capacitance matching of the dual-rail data outputs of each gate. Process variability and a lack of design tools make this requirement very difficult to satisfy in practice. We present a novel asynchronous dual-rail gate design which is power balanced and capable of tolerating interconnect variability. Additionally, its asynchronous nature allows for further tolerance to timing constraints and the asynchronous operation simplify secure, power balanced design.**

I. Introduction

Power analysis attacks exploit minute data-dependent power signatures of circuits to non-invasively extract sensitive data, such as secret keys, from embedded hardware [1] [2]. A promising countermeasure against these attacks has been based on gate-level power balanced designs. The goal of the countermeasure is to balance each logic cell such that the instantaneous power consumption is equal for all processed logic values and transitions to ensure that it does not produce a data-dependent power signature which can be used in an attack. The gate-level granularity of the method allows easy application to many different designs and the distributed nature of the countermeasure makes it harder for an attacker to circumvent.

Several designs of balanced gates have been proposed (SABL [3], DyCML [4], WDDL [5], Dual-Spacer [6]). The proposed designs differ slightly as to the level of balance they provide and their exact design objectives but all the proposed designs are based on dual-rail return-to-zero (RTZ) type implementations to ensure balanced operation at the logical outputs of the gates. The protocol implemented at the outputs of the gate represents each logic value with two rails which reset to a constant value prior to switching. In principle, the dual-rail and RTZ combination guarantees a constant Hamming weight of data and data-independent switching at the output of the gate.

However, in the existing designs the data-independent power consumption can only be guaranteed if the capacitances of each of the outputs of a dual-rail pair are perfectly matched. The dependence on matching capacitances of each dual rail pair is the major limitation of the practicality and feasibility of the designs due to the sub-optimality of interconnect routing tools and the unavoidable variation due to manufacture.

We present gate designs which have data-independent power consumption in the presence of inevitable interconnect imbalances which can result from routing and process variability. The gate designs, which we call asynchronous directional latch based logic (ADLBL) achieve data-independent power consumption with a dual-rail directional discharge protocol that does not require balanced routing of the dual-rail wire pairs. The proposed gates use delay insensitive asynchronous design eliminating clocking and timing problems associated with some previous dynamic designs.

II. Design Overview

The design philosophy of the proposed designs is based on two main trends associated with deep-submicron technology. First, as features of devices are scaled the gate interconnect has become a dominant source of dynamic power consumption, overshadowing that due to the intrinsic gate capacitances. Secondly, intra-die variations are generally small within an area of a single logic cell. Unlike previous designs which achieve balanced operation by matching load capacitances and concentrating on balancing internal operation our designs concentrate mainly on the communication protocol which is the major source of dynamic power consumption and variability. To illustrate the proposed design we start with the general communication protocol.

The design is based a dual-rail RTZ data communication protocol and a uses a component that we call a directional latch (DL) which allows complete discharge of both rails of the dual-rail pair. The directional latch is a circuit which can sense the directional discharge of the dual-rail input. Depending on the direction of discharge, the circuit latches an appropriate logical value into the gate.

Without a loss of generality, consider the signaling of a one-bit value between two buffers. The method of communicating a bit value with constant power using a directional latch between two buffers is shown in Figure 2 and uses two wires for each bit. Unlike the previous designs, the data bit is not communicated by charging one of the two rails but instead a value is communicated by pulling down one of the precharged rails. Pulling down one rail causes the discharge of the other rail through the directional latch. The directional latch can sense which rail initiated the discharge and the bit value can be determined by the receiving gate.

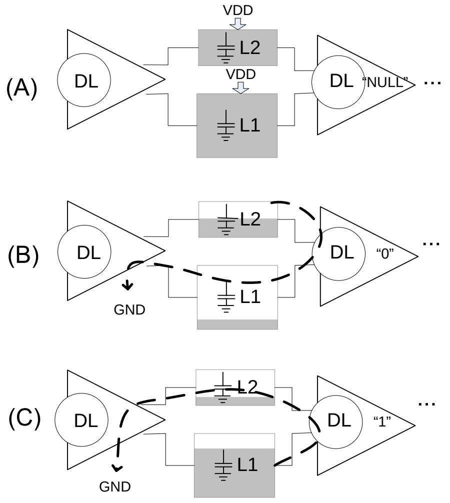


Fig. 1. Dual-rail protocol based on a directional latch

The general proposed operation which assumes a dynamic logic style implementation and achieves routing independent balance is as follows:

1) *Precharge phase*. (Figure 1a) All gates and interconnect are precharged to a high value.
2) *Evaluate phase*. (Figure 1b and Figure 1c) One rail of a dual rail pair is pulled low. The other rail of the dual-rail pair is directionally discharged through the directional latch. The directional latch senses the direction of the discharge and latches the appropriate value which can be used to implement the Boolean functionality.

Using this communication protocol both rails of a dual-rail pair get equally charged and completely discharged for each cycle regardless of the data. Since both rails are involved in both the precharge and evaluate cycles, the total capacitance charged and discharged is always constant and is independent of the relative capacitance values of a dual-rail wire pair.

III. Implementation

A hierarchical description of a complete single input ADLBL gate (buffer) is shown in Figure 2. The gate consists of the main datapath composed of a directional latch (for each dual-rail data input) and the pulldown network (PDN) which implements the Boolean functionality. The gates are wrapped with the asynchronous control circuitry which is composed of a Muller C-element (C) [7] and a completion detector in the form of a NOR gate. The ADLBL asynchronous wrapper is based on a modification of the asynchronous precharge half buffer template [8] [11].

The directional latch translates the directional discharge protocol at the input to the gate into stable differential dual-rail signals which are the inputs to the pulldown network. A possible design for the directional latch is based on a sense amplifier (SA) (Figure 3a) which is shown with the precharge transistors (M2, M3). The sense amplifier has a pass transistor (M1) between the two data rails which allows the directional discharge of both rails. During evaluation the voltage difference between the rails caused by the directional discharge will force the cross coupled inverters of the SA to latch a stable output which serves as the input to the PDN.

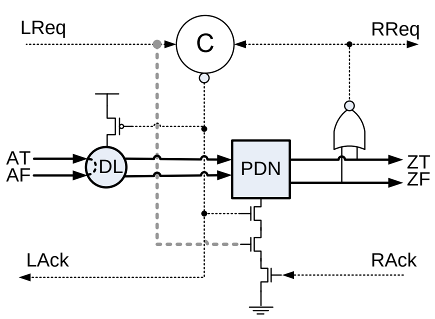
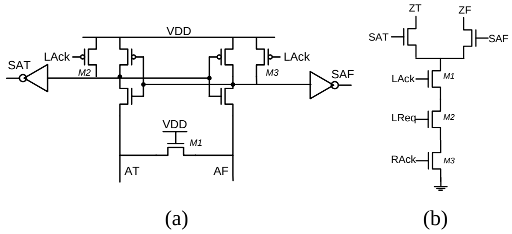


Fig. 2. Hierarchical design of an ADLBL gate

The PDN is a traditional differential NMOS pulldown network which pulls down one of the output rails depending on the desired function. The PDN for a buffer is shown in Figure 3b with the gate transistors (M1,M2,M3) shown which are used by the asynchronous wrapper to control the timing of the discharge.

The asynchronous wrapper controls the handshaking and transfer of data between gates removing the need for global clocking or control. Each gate can accept, process and output data on the basis of local handshaking. Because the signals generated by each gate allow it to accept and process data only when it is ready, the circuit is able to self-time its own operation. This style of design is also called micropipelining or fine grained pipelining as each gate behaves almost like its own pipeline stage and can tolerate large timing and voltage variations [8] [11].



(a) (b)

Fig. 3. (a) Sense amplifier as a direction latch (b) pulldown network of a buffer

The simulated timing diagrams for an ADLBL buffer, which has all of the same control signals as any other gate, is shown in Figure 4. The same timing and signal relationship exists for any ADLBL gate. The timing diagrams are from SPICE simulations for designs based on a 0.18um TSMC technology. Figure 4 has two sets of curves, black and gray. The black curves are the signals which interface with the fanout gate (ZT,ZF,RReq,RAck) while the gray curves are for signals which interface with the fanin gate (AT,AF,LReq,LAck)(from Figure 2). The two sets of signals (black and gray) are delayed copies of each other since the fanin signals are the fanout signals for another gate. For clearer explanation, we divide the operation of the gate into a precharge phase and a discharge phase with respect to the output of the buffer.

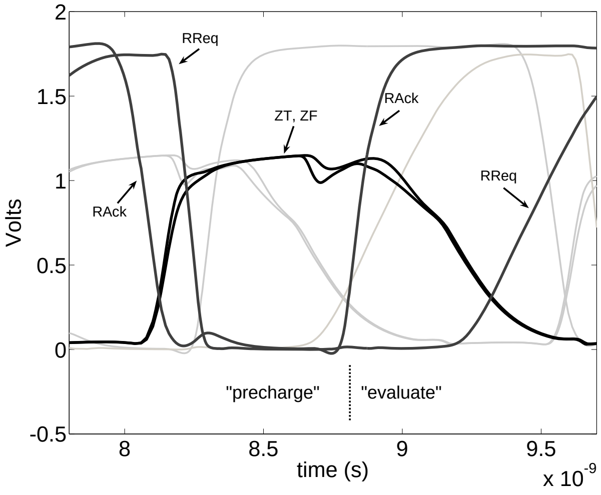


Fig. 4. Timing of signals

The precharge phase begins when the RAck signal of the fanout gate falls low. The falling RAck signal enables the sense amplifier of the fanout gate to precharge the rails. During this time the LAck signal of the local gate is low which prevents the simultaneous discharge through the PDN. As the rails are precharged through the sense amplifier of the fanout gate the completion detection (NOR gate) of the local gate pulls down the RReq signal. When the fanout gate completes its evaluation phase the RAck signal goes high stopping the precharge of the rails. As RAck rises it also starts the evaluation phase of the local gate as LAack is high and LReq is low. The pulldown network starts discharging both rails by pulling one low, hence there is a small lag between the discharge speed of the two rails. This difference causes the sense amplifier to latch the value. As the two rails are pulled to ground the completion detection output, RReq, goes high and stops the evaluation.

In both the evaluate and precharge phases there is a small lag during the discharge and charge between the dual-rail wire pairs. This lag is necessary for our design as we require a voltage drop across the pass transistor to latch a value into the sense amplifier. The time lag can translate into shorter or longer discharge times depending on which rail is pulled low if the routing capacitances are significantly imbalanced. However, even under extreme capacitance mismatch (50x), the time differences of discharge times are in the order of picoseconds. Such differences cannot be reliably measured outside of a chip due to the large capacitances of the power and ground rails. We note that this lag or "exposure time" [6] is several orders of magnitude smaller than in previous designs. We therefore consider this lag to be negligible but the feasibility of exploiting temporal differences of this magnitude is under investigation.

IV. Balance Analysis

The balance of the proposed designs was evaluated and compared with WDDL and SABL gate styles. Analysis was performed for individual gates and for a subcircuit of the Advanced Encryption Standard (AES). In both analyses the output capacitances of the dual rail data pairs were mismatched and differences in power and energy consumption for different data values were compared. In all analyses performed, the power consumption of the proposed designs was independent of the interconnect mismatch. The ADLBL gates maintained their balance, and hence their security, despite very large capacitance mismatch of the dual-rail data pairs. The balance and security of the other two styles was completely dependent on the matching of the output capacitances.

For example, Figure 5 shows the standard deviation (STD) of the energy for a two input NAND gate for all possible inputs as a function of the capacitance mismatch of the output of the gate. The Figure shows the results of SPICE simulations for the gate styles when one output rail was loaded with a capacitance of 2fF and the other with varying loads from 2fF to 26fF. The STD of energy for the proposed designs was invariant to the output mismatch. Similar simulations were performed analyzing the instantaneous power consumption for the different gates which showed similar results.

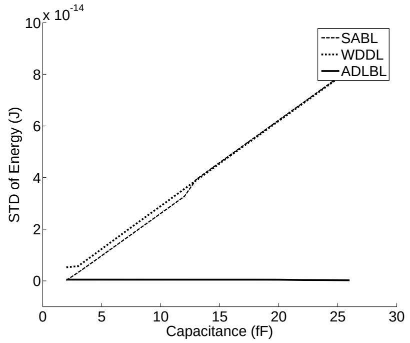


Fig. 5. Standard deviation of energy for NAND gates

Additional analysis was performed on a subcircuit of AES. A 4-bit input and 4-bit output combinational circuit which performs multiplicative inversion in $GF(2^4)$ (a subcircuit of AES SBox) was implemented with the ADLBL and WDDL gates. The interconnect within the circuit was loaded with capacitances such that the distribution of the ratios of capacitances of all dual-rail data signals pairs corresponded to a normal distribution with different variances. A correlation power analysis attack based on the Pearson's correlation coefficient was mounted against the two implementations. The differences in correlations between a correct key value and the highest correlation of an incorrect key is compared in Table I. Regardless of the variance of the ratio of the capacitance distributions the correlation power attack was unsuccessful against the ADLBL implementation. For the WDDL gate, however, the correct key was easier to distinguish from the other incorrect keys as the variance of the mismatch increased.

variance of capacitance ratios	difference of correlation	
	WDDL	ADLBL
0.05	0.6	0
0.08	0.9	0
0.1	0.1	0

TABLE I

EFFECT OF CAPACITANCE VARIANCE ON CORRELATION IN POWER ANALYSIS ATTACKS

V. ADDITIONAL DESIGN BENEFITS

A. Noise

The presented design features an additional transistor in the pull down network to prevent noise or glitches due to crosstalk from propagating during the evaluation phase of the gate. The extra transistor ensures that glitches amplified by the DL do not cause evaluation in the pulldown network. The transistor is controlled by the LReq signal from the fanin gate which is high only when both data rails have discharged. (Depicted by a gray dotted line in Figure 2.) The LReq signal is generated by the static NOR gate of the fanin gate allowing for dynamic noise margins on the data path which are similar to that of a static CMOS (SCMOS) gate.

The noise immunity curves comparing the dynamic noise margins for a ADLBL buffer and a SCMOS inverter are shown in Figure 6. Rectangular pulses were injected into the data inputs of varying amplitudes and widths in a SPICE simulation using minimal transistor sizing and a TSMC 0.18um technology. The Figure shows a line for each logic style for each pulse width above which the amplitude is considered the failing region. For the SCMOS inverter the amplitude of the input pulse amplitude is considered failing if it results in a pulse of larger or equal amplitude at the output of the gate (results in a gain of greater or equal than one). For the ADLBL buffer the input pulse amplitude was considered failing if it caused any effect at the output of the sense amplifier of the fanout gate. As can be seen from the figure the dynamic noise margins of the datapath of the ADLBL buffer are comparable to the noise margins of the static CMOS inverter despite the stricter definition of the passing region for the former.

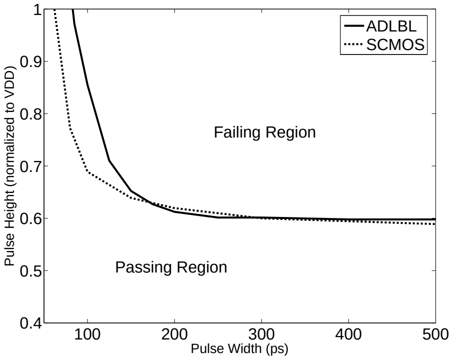


Fig. 6. Dynamic noise margins

B. Balance

The presented designs achieve balance on the inter-gate wires independently of their capacitive loads but internally the gates require careful design and layout to match the capacitances of internal dual-rail signals. Among the critical signals which require careful symmetric layout are the dual-rail outputs of the sense amplifier. This task is simplified by the inherent symmetry of the design. Each wire of a dual-rail pair sees the same capacitive loads. By using the design methodology presented in [10] the pulldown network was made symmetric such that each discharge path has the same depth and each input has the same load.

Additionally, due to the use of a NOR gate as the output completion detection each gate has a self-checking balance detection. It has been previously noted that many balanced gates can have untestable manufacturing defects or faults which can cause imbalances allowing power attacks [9].

To ensure balance, the ADLBL protocol requires that both data rails of each gate are charged and discharged for each cycle. For the proposed ADLBL gates the handshaking protocol of the design will fail and the gate will deadlock in case of failure to discharge both data rails for each data cycle. The handshaking circuitry propagates any failures of the balancing protocol into the datapath making such failures stop the circuit regardless if they were natural or due to an attacker.

VI. CONCLUSION

The ADLBL gates maintain their balanced operation despite capacitance mismatch of their dual-rail outputs. The asynchronous operation allows for self timed operation and serves a self checking mechanism capable of detecting failures which can lead to imbalances, provides additional security benefits, and allows an automated design flow [11].

REFERENCES

[1] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," CRYPTO, 1999.

[2] S. Mangard, E. Oswald and T. Popp, *Power Analysis Attacks, Revealing the Secrets of Smart Cards*, Springer, 2007.

[3] K. Tiri, M. Akmal and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards," ESSCIRC pp. 403-406,2002.

[4] F. Mace, F.X. Standaert, J.J Quisquater and J.D. Legat, "A Design Methodology for Secured ICs Using Dynamic Current Mode Logic," PATMOS, pp. 550-560, 2005.

[5] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," DATE, pp. 246-251, 2004.

[6] D. Sokolov et al., "Improving the Security of Dual-Rail Circuits," CHES, pp. 282-297, 2004.

[7] J. Spars and S. Furber (eds.), *Principles of asynchronous circuit design. A systems perspective*. Kluwer Academic Publishers, 2002.

[8] R.O. Ozdag and P.A. Beerel, "High-Speed QDI Asynchronous Pipelines," ASYNC, pp. 13-22, 2002.

[9] K.J. Kulikowski, M. Karpovsky, A. Taubin, "DPA on Faulty Cryptographic Hardware and Countermeasures." FDTC,pp. 211-222, 2006.

[10] K. Tiri and I. Verbauwhede, "Design Method for Constant Power Consumption of Differential Logic Circuits," DATE, pp. 628-633, 2005.

[11] K.J. Kulikowski, A. Smirnov and A. Taubin, "Automated Design of Cryptographic Devices Resistant to Multiple Side-Channel Attacks", CHES, pp. 339-413, 2006.