Charge Recycling Sense Amplifier Based Logic: Securing Low Power Security IC's against DPA

Kris Tiri[1] and Ingrid Verbauwhede[1,2]
[1]UCLA Electrical Engineering Department, [2]K.U.Leuven
{tiri, ingrid}@ee.ucla.edu

Abstract

A Charge Recycling Sense Amplifier Based Logic is presented. This logic is derived from the Sense Amplifier Based Logic, which is a logic style with signal independent power consumption. It has been proven previously to protect security devices such as Smart Cards against power attacks. Experimental results show that the use of advanced circuit techniques, which enable charge recycling and intermediate precharge voltages, saves 20% in power consumption and 63% in peak supply current and that the logic style preserves the energy masking behavior of the Sense Amplifier Based Logic.

1 Introduction

Security is as strong as the weakest link. Strong encryption algorithms have been designed to withstand cryptanalysis that has access to plaintext and ciphertext. The physical implementation however, provides the attacker with important extra information. Numerous attacks have been presented that use 'side channels', such as time delay and power consumption, as an extra source of information to find the secret key. Especially the Differential Power Analysis (DPA) [1] is of great concern. It is very effective in finding the secret key and can be mounted quickly with off-the-shelf devices. The attack is based on the fact that logic operations have power characteristics that depend on the input data and the secret key. It relies on statistical analysis to extract the information from the power consumption patterns.

At first, the DPA has been fought with ad hoc countermeasures. For instance, the addition of random power consuming operations obscured the data dependent variations in the power consumption [1]. Yet over time, the attacks have evolved and become more effective. To address the problem, countermeasures need to be provided at different design abstraction levels. At the algorithmic level, a fine illustration is masking [2]. This technique prevents intermediate variables to depend on an easily accessible subset of the secret key.

Only recently, at the circuit level, dedicated hardware techniques have been proposed [3],[4]. Instead of concealing or decorrelating the side channel information, these techniques aim at not *creating* any side channel information. Goal of these countermeasures is to balance the power consumption of the logic gates. When the power consumption of the smallest building block, i.e. a logic gate, is independent of the signal activity, no information is leaked through the power supply regardless of the data or secret key being processed. One such logic style is Sense Amplifier Based Logic (SABL) [5].

Most wireless embedded applications have cryptographic capabilities for authentication and confidentiality. For these battery-powered devices much focus is on lower power design. We have analyzed advanced circuit techniques to reduce the power consumption of SABL.

SABL is a precharged and differential logic style. Because of this, is does consume a substantial amount of power. The Charge Recycling SABL (CRSABL) recycles the charge stored at one output node in the evaluation phase to partially charge the output and the internal nodes to an intermediate voltage in the next precharge phase. This technique achieves a reduction in power consumption of 20%. Since CRSABL reuses internally stored charge, it also benefits from a reduction in the supply current derivative *di/dt* and the peak supply current. As a result, the supply bounce, often a critical problem for signal integrity, is lowered. Furthermore, CRSABL reduces the number of clocked transistors with one third.

Section 2 describes CRSABL. The discussion consists of (1) an introduction to SABL, (2) a description of the CRSABL inverter, (3) design rules for cascading charge recycling dynamic gates, (4) the energy-delay performance and (5) techniques to overcome destructive charge sharing effects in arbitrary CRSABL gates. In section 3, an experiment is setup to compare the performance and energy masking behavior of CRSABL and SABL. Finally a conclusion will be given.

2 Charge Recycling SABL

2.1 SABL

Sense Amplifier Based Logic is a logic style that uses a fixed amount of charge for every transition, including the degenerated events in which a gate does not change state. In every cycle, a SABL gate charges a total capacitance with a constant value.

SABL is based on 2 principles [5]. First, it is a dynamic and differential logic style and therefore has exactly one switching event per cycle and this independently of the input value and sequence. Since a differential logic family uses the true and the false representation of the in- and output signals and a dynamic logic family alternates precharge and evaluation phases, both outputs are precharged to 1 in the precharge phase and exactly 1 of the 2 outputs evaluates to 0 in the evaluation phase.

Second, during a switching event, it guarantees that the load capacitance has a constant value. SABL completely controls the portion of the load capacitance that is due to the logic gate. The intrinsic capacitances at the differential in and output signals are symmetric and additionally it discharges and charges all the internal node capacitances trough a special pull down network.

2.2 Inverter

The SABL and the CRSABL inverters are depicted in Figure 1 (left and right). The gates differ in one essential point. The two clocked pmos transistors that precharge the output nodes of the SABL inverter to the supply voltage VDD, are replaced by one clocked pmos transistor between the output nodes of the CRSABL inverter.

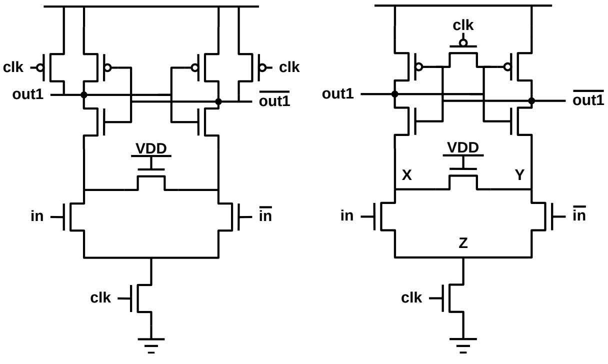

Figure 1. Inverter: SABL (left); and CRSABL (right)

Figure 2 shows a switching event of the CRSABL inverter. At the onset of the precharge phase (clk-signal low), node Z is disconnected from GND and the output nodes are shorted. The high output drops and the low output rises in order to converge to the same voltage, which is VDD – $|V_{tp}|$. V_{tp}, V_{tn} are the threshold voltages. At that moment, the pmos transistors of the cross-coupled inverter are turned off. Meanwhile, the internal nodes X and Y have been precharged to VDD – $|V_{tp}|$ – V_{tn}. During the subsequent evaluation phase (clk-signal high), the gate will evaluate to a differential output as soon as one transistor of the differential input pair provides a path to GND.

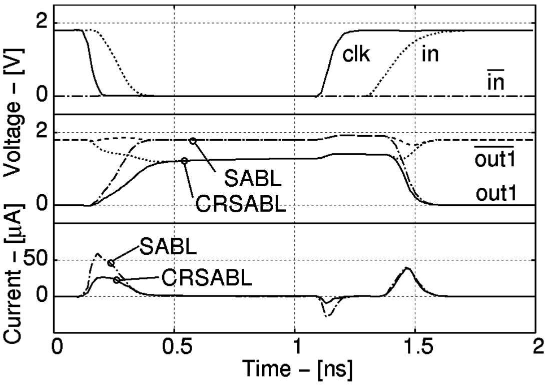

Figure 2. Simulated waveform transients of inverter: input (top); output (middle); and current (bottom)

Figure 2 also shows a switching event of the SABL inverter for the same inputs. CRSABL has both a lower total power consumption and a smaller peak current. The transistor sizes of both gates are optimized for minimum power consumption.

CRSABL consumes less power for two reasons. The first effect is charge recycling. The charge stored on the high output node during the evaluation phase is used to partially charge the low output node during the precharge phase. As a result, less charge has to come from the power supply. Secondly, the output and the internal nodes are only precharged to VDD – $|V_{tp}|$ and VDD – $|V_{tp}|$ – V_{tn} respectively. This is one threshold voltage below the precharge voltages of SABL. Since one output and all internal nodes, are discharged in every cycle, the lower the precharge voltages are, the lower the power consumption will be.

The peak supply current is smaller not only because less charge is required but also because the precharge current is no longer supplied by clocked transistors, which are entirely open and provide a high peak current.

2.3 Cascading Gates

CRSABL, like SABL, is a dynamic logic style. Dynamic logic is connected using either domino logic, in which each gate is extended with a pair of inverters, or np-logic, in which n- and p-type gates are alternated.

CRSABL can never be connected according to the np-logic rules. The output signals of the p-type gate are pre-'dis'-charged to V_{tn}. In this regime, the input transistors of the subsequent n-type gate have a very high leakage current. The charge on the output nodes would quickly leak away and the cross-coupled inverter would switch. Furthermore, any noise disturbance turns the transistors on and accelerates the process.

Consequently, CRSABL can only be cascaded using domino logic. Yet, static inverters should not be used for the same leakage reason. They suffer from a direct path current when their input is at VDD – $|V_{tp}|$. There are circuits that recover a full swing at the output without direct path current. Figure 3 (left) uses a high V_t pmos transistor. While this requires extra masks and processing steps, more and more designs nowadays use high V_t transistors to control subthreshold currents. Figure 3 (middle) [6] uses an enable signal to stop the direct path current. This requires 1 additional transistor and the generation of the enable signal. Finally, the circuit in Figure 3 (right) [6] consists of only 2 regular transistors driven by both output signals. This circuit has poor drive strength, as the current does not directly come from the supply.

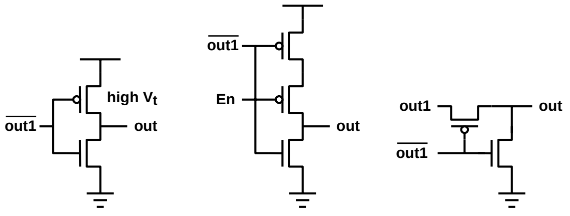

Figure 3. Circuits to recover a full swing without direct path current

2.4 Performance

This section compares the energy-delay characteristics of CRSABL and SABL. Two circuits are implemented: a CRSABL inverter extended with the circuit of Figure 3 (right) at both output nodes; and a SABL inverter extended with a pair of static inverters. The circuits are implemented in a 0.18µm, 1.8V CMOS technology. Simulations are done in HSPICE.

Detailed SPICE simulations are done with the setup depicted in Figure 4 [7]. Four measurements are reported. E_{int} includes the power dissipated when the internal nodes of the gate switch, but excludes the power dissipated on the load capacitance. E_{data} and E_{clk} present the portion of the gray and black inverters' power consumption dissipated in the gate. Finally, the delay is measured between the 50% transition points of the input and output in the evaluation phase. The delay in the precharge phase is insignificant. All gates precharge in parallel. Note that the power measurements reflect precharge and evaluation phase.

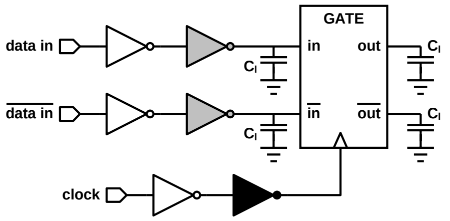

Figure 4. Measurement setup

Figure 5 shows the minimum energy-delay curves for C_l equal to 10fF as a function of the transistor sizes. SABL achieves a lower minimum Energy Delay Product (EDP) then CRSABL. The minima are 7.2e-24 and 10.4e-24 respectively. For Smart Card applications however, speed performance is not important. Most Smart Cards have an internal clock frequency ranging from 10 to 20 MHz. Current state-of-the-art has a maximum internal clock frequency of a mere 55MHz [8]. For Smart Cards and battery-operated devices, the energy consumption per cycle, aka the Power Delay Product (PDP), is a better measure. CRSABL achieves 25.7fJ compared to 34.3fJ for SABL.

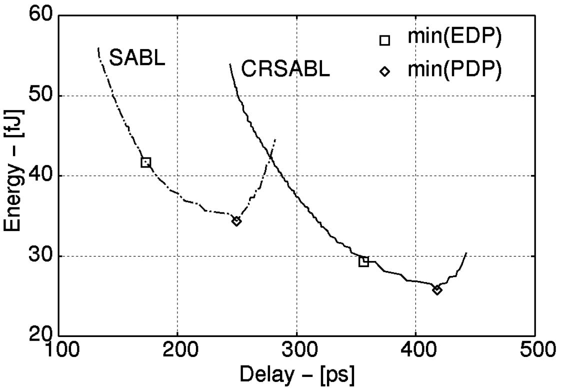

Figure 5. Energy-delay tradeoff of inverter

Table I summarizes the energy-delay characteristics for the circuits with minimum PDP. A reduction of the clock load from 3 to 2 transistors has saved 41% in E_{clk}. E_{int} and E_{tot} have been reduced with 24% and 25% respectively. The tradeoff is with an 68% increase in delay.

Table I. Energy-delay characteristics of inverter

	E_{int} (fJ)	E_{data} (fJ)	E_{clk} (fJ)	E_{tot} (fJ)	delay (ps)
SABL	28.7	0.7	5.0	34.3	249
CRSABL	21.9	0.9	2.9	25.7	418

2.5 Charge Sharing Effects

CRSABL gates are built by replacing the input differential pair with a differential pull down network (DPDN). A special DPDN that for a differential input connects all internal nodes to an output node should be used to achieve constant power consumption [5]. Figure 6 (left) shows the CRSABL AND-gate extended with a designated circuit at its outputs to recover full swing.

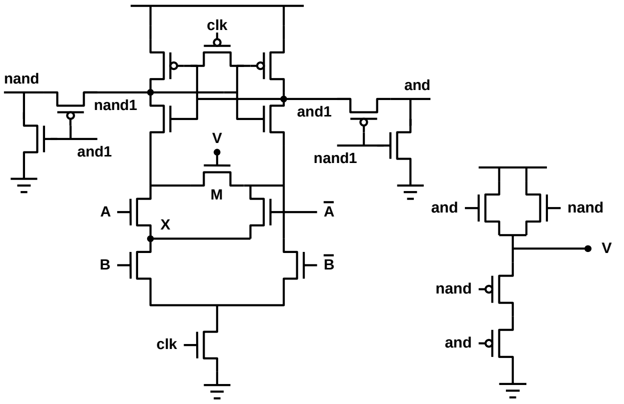

Figure 6. AND gate (left); and feedback network (right)

This circuit however, suffers from charge sharing, which is a result from incompletely loaded internal nodes. Figure 7 (top) and (middle) show how this can lead to failure. Worst-case charge sharing occurs when the input signals, i.e. A, $\overline{A}$, B and $\overline{B}$, have been precharged to 0 before the falling edge of the clock. Note that this situation happens if there is a large jitter on the clock such that all gates do not precharge exactly at the same moment. When A becomes 1, charge from node nand1 will be used to charge node X. Note that node X is disconnected from GND as B and $\overline{B}$ are still at 0. As a result, the cross-coupled inverter, which was in a metastable state, will choose side. If subsequently $\overline{B}$ becomes 1 the cross-coupled inverter keeps its state and the gate produces an incorrect output.

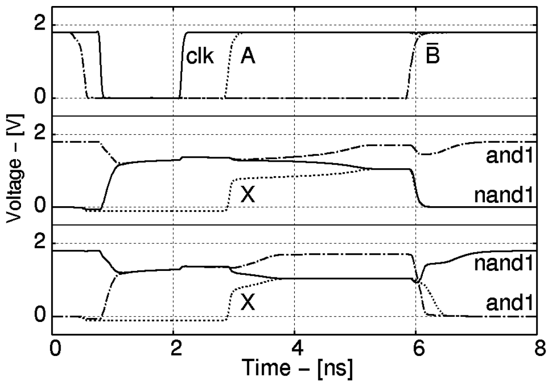

Figure 7. Simulated waveform transients: input (note: $\overline{A}$ = 0, B = 0 throughout entire transient) (top); output (middle); and output with feedback (bottom)

SABL also experiences destructive charge sharing. Here, the remedy consists of increasing the length and thus the resistance of transistor M_1. This decreases the gain in the feedback loop. The result is that node and1 can discharge, compensate for the drop in nand1 and switch the cross-coupled inverter back to the other site. This is not a viable solution for CRSABL as the length of M_1 would become too large. Because of the lower precharge voltage, the voltage difference between nodes and1 and nand1 after charge sharing is too significant.

The resistance of M_1 can also be increased by applying a low bias voltage V such that transistor M_1 is only turned on to close the feedback loop of the cross-coupled inverters whenever its drain or source is almost at 0. The shortcoming of this approach is that a bias voltage needs to be distributed to all gates. A better solution is to use the feedback network depicted in Figure 6 (right). This circuit will turn on transistor M_1 when 1 output node has become 1. Figure 7 (bottom) shows the output voltages of the CRSABL AND-gate with feedback network. Simulations indicate that the feedback network does not result in a delay penalty.

3 Cell library and application

We have built a set of basic gates and implemented a typical cryptographic function in HSPICE in order to evaluate CRSABL with respect to the energy-delay performance and energy masking behavior of SABL. All gates are connected in domino fashion and have been optimized for minimum PDP. The CRSABL gates use the feedback network and the SABL gates an appropriate sizing of transistor M_1 to avoid destructive charge sharing effects. Measurements have been performed according the technique described in section 2.4.

The basic gates are the AND- and XOR-gate. This is a sufficient set to implement any logic function. The differential inverter is redundant as differential logic has both the true and the false output. The OR-gate is derived from the AND-gate by exchanging the inputs. Table II, which has been derived for a C_l of 10fF, shows that there is reduction of roughly 25% in E_{tot}. The delay increase is around 43%.

Table II. Energy-delay characteristics basic cells

	AND		XOR	
	E_{tot} (fJ)	Delay (ps)	E_{tot} (fJ)	Delay (ps)
SABL	**42.7**	**312**	**48.7**	**325**
CRSABL	**33.1**	**452**	**35.5**	**459**

With these cells we have implemented the S9 substitution box of the Kasumi algorithm, the encryption algorithm in the 3G cellular standard [9]. After synthesis, the module has a maximum logic depth of 5 and consists of 86 XOR- and 46 AND-gates.

Table III summarizes the simulation results. The reduction of 20% in E_{tot} comes from a combined reduction of 18% in E_{int} and 43% in E_{clk}. There is an increase of 34% in the delay of the module. CRSABL preserves the energy masking behavior of SABL. Both, the normalized absolute variation of the energy per cycle (NED) and the normalized standard deviation of the energy per cycle (NSD), are small.

Figure 8 shows the statistical properties of the instantaneous supply current. The mean current is a representative switching event. The point wise absolute variation and standard deviation are small throughout the entire event. Note that both logic styles have a comparable absolute variation and standard deviation. This is important since the attacker is not so much interested in the total charge per switching event, as he is in the instantaneous current. He will sample several times per clock cycle to capture the instantaneous current. The increase in relative energy variation in Table III is mainly the effect of a reduction of the normalization factor, which is the mean energy consumption. Note also that the peak supply current drops from 8.9mA to 3.3mA, a reduction of 63%.

Table III. Energy-delay characteristics of S9box

	NED (e-3)	NSD (e-7)	E_{tot} (pJ)	delay (ps)
SABL	**5**	**5**	**5.94**	**696**
CRSABL	**13**	**11**	**4.75**	**932**

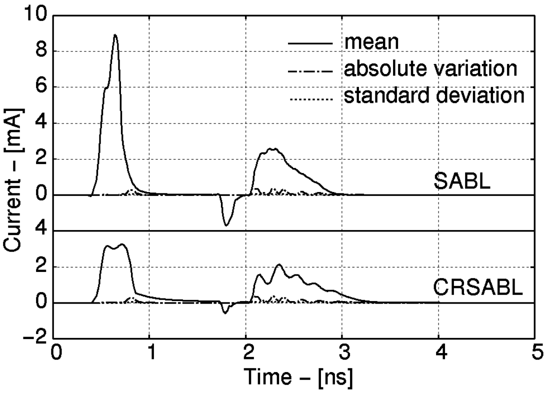

Figure 8. Typical supply current of S9box

4 Conclusions

We have presented a logic style to secure low power security IC's against differential power analysis. Experimental results have shown that through charge recycling and lower precharge voltages, Charge Recycling SABL achieves a 20% reduction in the total power consumption and a 63% reduction in the peak supply current of SABL. CRSABL preserves the resistance of SABL against power attacks.

Acknowledgements

The authors would like to acknowledge the support of the National Science Foundation (CCR-0098361).

5 References

1. P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," Proc. of Advances in Cryptology, pp. 388-397, 1999.
2. S. Chari, C. S. Jutla, J. R. Rao and P. Rohatgi, "Towards Sound Approaches to Counteract Power-Analysis Attacks," Proc. of CRYPTO'99, LNCS 1666, pp. 398-412.
3. J. Fournier, S. Moore, H. Li, R. Mullins and G. Taylor, "Security Evaluation of Asynchronous Circuits," Proc. of CHES 2003, LNCS. 2779, pp. 137-151.
4. K. Tiri and I. Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology," Proc. of CHES 2003, LNCS 2779, pp. 125–136,.
5. 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," Proc. of ESSCIRC 2002, pp. 403-406.
6. B. Kong, J. Choi, S. Lee and K. Lee, "Charge Recycling Differential Logic (CRDL) for Low Power Application," IEEE JSSC, vol. 31, pp. 1267–1276, 1996.
7. V. Stojanovic and V. G. Oklobdzija, "Comparative analysis of masterslave latches and flip-flops for high-performance and low-power systems," IEEE JSSC, vol. 34, pp. 536–548, 1999.
8. SLE88CX720P Short Product Information, http://www.infineon.com, June 2003.
9. Specification of the 3GPP confidentiality and integrity algorithms, http://pda.etsi.org/pda, June 2002.