Available online at www.sciencedirect.com
ScienceDirect
INTEGRATION, the VLSI journal 40 (2007) 355–364
INTEGRATION the VLSI journal
www.elsevier.com/locate/vlsi

Dynamic differential self-timed logic families for robust and low-power security ICs

Ilham Hassoune*, Francois Mace, Denis Flandre, Jean-Didier Legat

Microelectronics Laboratory, Université catholique de Louvain (UCL), Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium

Received 9 November 2005; received in revised form 8 March 2006; accepted 15 April 2006

Abstract

This paper describes two new dynamic differential self-timed logic families that can be used either to implement low-power security components or low-power high-speed self-timed circuits. Electrical simulations in 0.13 μm partially depleted (PD) SOI CMOS under a V_{dd} of 1.2 V have shown that the substitution box (S-box), a module of the Khazad cipher algorithm, implemented with the improved feedback low swing current mode logic (IFLSCML) features a power consumption standard deviation almost five times smaller than that of the self-timed DDCVSL one, while consuming 37% less. On the other hand, the 8b CLA implemented with dynamic differential swing limited logic (DDSLL) features a power delay product about 19% lower than that of its counterpart implemented with self-timed DDCVSL.

Keywords: Self-timed logic; Low-power; Differential power analysis; DPA; Secure smart cards

1. Introduction

Securing implementation of encryption algorithms at the hardware level has gained importance in the research community, particularly as the hardware implementation may leak information about the encrypted data through side-channel attacks (SCAs). Among these attacks, power analysis attacks that rely on measurements of instantaneous power consumption and statistical analysis are cheap and easy to mount. As a consequence, there is a growing focus of cryptographers and hardware designers on the material security issue. Several works have proposed solutions to balance power consumption and reduce the data-dependent power signature at architecture and logic levels. Nevertheless, many achieve this goal by introducing dummy logic blocks or dummy transistors, which significantly increases both power consumption and area and degrades speed performance.

In this paper, we propose a new class of low swing current mode logic families that feature a dynamic differential self-timed nature. Two implementations are proposed, namely LSCML and dynamic differential swing limited logic (DDSLL). They are evaluated in terms of security and robustness against power analysis attacks, but also in terms of speed performance and power consumption that are crucial in data-path circuits.

2. Power-aware design criteria

Over the last 20 years, asynchronous architectures and systems have raised a great deal of interest in the research community. Due to the rapid growth of chip sizes and packing, it becomes difficult to synchronize perfectly all the parts of Systems-on-Chips (SoCs). On the other hand, design of clock distribution trees for synchronous systems will not possibly be optimized anymore to be tailored to multi-GHz frequencies. Hence, asynchronous architectures are becoming necessary to avoid synchronization failures while allowing more design flexibility than synchronous architectures [1].

For power-aware applications, clock-gating and asynchronous design have often been reported as an effective way to save power at the architecture level [1–3], as each logic unit is enabled only when necessary. Surely the gain in

*Corresponding author. Tel.: +32 10 47 25 40; fax: +32 10 47 25 98.
E-mail address: hassoune@dice.ucl.ac.be (I. Hassoune).

0167-9260/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.vlsi.2006.04.001

power consumption can better be obtained in asynchronous systems than in synchronous ones though it remains application-dependent since the overhead circuitry due to the handshaking protocols increases the power in asynchronous SoCs. Nevertheless self-timed architectures offer a large flexibility to designers as it allows a local optimization independently of the external clock-frequency [1]. Self-timed operation has particularly been suggested to take advantage of the data-dependency in applications where arithmetic data processing is dominant.

At the logic level, besides the lowering of supply voltage, the use of a low power library, the capacitance reduction and the use of multi-threshold circuit techniques (MTCMOS), reducing the output voltage swing is another way to save power [4–6].

3. Security ICs criteria

During last decades, a large amount of work has been done on cryptographic hardware to ensure that security features obtained at the algorithmic level would not be decreased by un-careful physical implementations of cryptographic primitives. Indeed, it could be emphasized that information about secret data handled by cryptographic circuits could leak from these devices under various forms, among which timing features, electromagnetic radiations or power consumption patterns are a few of them. These are known as side-channel leakage of information. To withstand this phenomenon, various countermeasures were developed at different levels of the design. Among all of them, those acting at the logical level seem to be interesting since they tackle the problem directly at its source.

3.1. Self-timed design to prevent DPA

If self-timed design has been found promising to implement low-power high-speed embedded systems, it demonstrated a great potential at the hardware level in the cryptography community as well. Actually, asynchronous designs have often been proposed to reduce SCAs attacks [7,8]. Differential power analysis (DPA) is the most powerful among these SCAs. However, whereas it has been well studied for synchronous designs [8], in asynchronous designs, there is no global clock to take as timing reference. As each individual circuit in the chip has its local self-timing, and thus operates independently of the global clock, the operation of individual units is consequently masked. This makes the power analysis cracking much harder for the attacker [8].

3.2. Dynamic differential logic to prevent DPA

Dynamic differential logic styles have been proposed to balance power consumption and reduce the data-dependent power signature. Kocher et al. were the first to demonstrate that instantaneous power consumption measurements of a smart card may reveal the sequence of instructions executed (simple power analysis or SPA) [9]. Furthermore, they may reveal the activity of a single gate (DPA). It has been shown afterwards in many works [10,11] that making the power consumption of security devices independent of the processed data helps to prevent power analysis attacks. Dynamic differential logic styles have been proposed as a solution to balance power [12]. To make it clear, let us examine the expression of the average dynamic power consumption [13].

$$P\mathrm{dyn} = \alpha_{0\to1} C_L V_{\mathrm{dd}} V_{\mathrm{swing}} f, \tag{1}$$

where C_{L} is the total parasitic capacitance, V_{dd} the supply voltage, V_{swing} the output logic swing ($V_{\mathrm{swing}} = V_{\mathrm{dd}}$ in full-swing logic families, V_{swing} is denoted ΔV in the rest of the text), f the clock frequency and $\alpha_{0\to1}$ the activity factor. The value of $\alpha_{0\to1}$ depends on different components that are the type of logic style, the type of logic function, circuit topology, signal statistics and the sequencing of operations [14]. $\alpha_{0\to1}$ is defined as the probability of an output transition $0\to1$. Let us assume a 2-inputs NOR gate with uniformly distributed and random inputs. For a NOR gate implemented in static CMOS, $\alpha_{0\to1} = 3/16$. The same gate implemented in a dynamic logic style gives $\alpha_{0\to1} = 3/4$, while its implementation in dynamic differential logic gives $\alpha_{0\to1} = 1$. Hence, dynamic differential gates ensure one output transition every cycle and this independently of the data inputs. Nonetheless, this is achieved at the expense of high power consumption due to the 100% switching activity. Reducing the output swing can help to reduce the dynamic power. On the other hand, it was shown in [15,16] that all dynamic differential logic styles are not equal in terms of robustness against power analysis attacks. Other factors like the total amount of the capacitance at the switching nodes and the circuit topology may make the difference.

To balance the total amount of the capacitance, authors in [16,17] have proposed sense amplifier based logic (SABL), which is a dynamic differential logic that uses a NMOS transistor which is always ON between the differential outputs in order to discharge all the internal node capacitances whatever the discharging node, and to transform asymmetric NMOS networks of logic functions like a AND/NAND gate by modifying the internal connections and adding dummy transistors. This results in an enhanced security at the expense of a significant increase in power consumption.

MOS current mode logic (MCML) [4] (Fig. 1) can also be an efficient way to prevent power analysis attacks. MCML gates consist in a differential pair operating with a constant current source. MCML gates feature a current mode operation and small output voltage swing. The power dissipation in MCML gates is constant as it is given by $V_{\mathrm{dd}} I$ where V_{dd} is the supply voltage and I is the constant current. The drawback of MCML gates lies in two details. First, the power consumption is independent of the operating frequency, which makes MCML logic advantageous