Microelectronics Journal 42 (2011) 180–187

Contents lists available at ScienceDirect

Microelectronics Journal

journal homepage: www.elsevier.com/locate/mejo

# The effectiveness of a current flattening circuit as countermeasure against DPA attacks

Haleh Vahedi *, Stefano Gregori, Radu Muresan

*School of Engineering, University of Guelph, Guelph, Ontario, Canada N1G 2W1*

ARTICLE INFO

*Article history:*
Received 31 January 2010
Received in revised form
9 August 2010
Accepted 11 August 2010

*Keywords:*
Current flattening
Current injection
Differential power analysis attack
Secure microsystems

ABSTRACT

This paper presents an on-chip current flattening circuit designed in 0.18-μm CMOS technology, which can be integrated with secure microsystems, such as smart cards, as a countermeasure against power analysis attacks. The robustness of the proposed countermeasure is evaluated by measuring the number of current traces required for a differential power analysis attack. We analyze the relationship between the required number of current traces and the dynamic current variations, and we show empirically that the required numbers of current traces is proportional to an inverse of the square of the rms value of the flattened current. Finally, we evaluate the effectiveness of the proposed design by using the experimental results of the fabricated chip. The analysis of the experimental results confirms the effectiveness of the current flattening circuit.



## 1. Introduction

With the proliferation of microsystems, especially smart cards, in applications, where security is a major concern, countermeasures protecting the secret key in microsystems have come to the forefront of research. Although the embedded nature of smart cards does not allow direct access to the secret key, acquiring the key through information extracted from the physical implementation is not impossible. In fact, such techniques of attacking smart cards, called side-channel attacks, are quite common and one of the most successful ones is the Differential Power Analysis (DPA) attack. In DPA attacks, statistical analyses are used for extracting information from dynamic variations of power or current in a cryptographic device [1].

Different approaches against DPA attacks, software- and hardware-based methods, have been discussed, among many, in [2–9]. Hardware-based countermeasures (circuit- and system-levels) were discussed in detail in [10]. Furthermore, the pros and cons of the existing techniques were reviewed there in the light of the key design challenge of combining the countermeasure effectiveness with low-power dissipation and small chip area. The results and analysis presented in [10] were based on simulations. This paper reports the effectiveness of the proposed countermeasure by means of the experimental results of the fabricated chip. Moreover the effectiveness of the countermeasure, previously evaluated in terms of the current attenuation, is here assessed in terms of its robustness against DPA attacks. The design, discussed in this paper, aims at proving the effectiveness of a specific current flattening technique based only on current injection and on an enhanced current sensor circuit.

The remainder of the paper is organized as follows. Section 2 illustrates the enhanced current flattening circuit. In Section 3, the functionality of the circuit is verified through simulations. In Section 4, the effectiveness in protecting smart cards against DPA attacks is evaluated by measuring the number of current traces required for a DPA attack. Also, the trade-off between power dissipation overhead and the degree of attenuation is discussed. Section 5 presents layout considerations and tests results for the fabricated chip. Finally, discussion and conclusion are covered in Section 6.

## 2. The enhanced current flattening circuit

The goal of the circuit shown by the block diagram of Fig. 1 is to keep the current flow through the power-supply terminal at a constant level.

The current sensor measures $I_S$ at the $V_{DD}$ terminal. The output $I'_S$ , an attenuated form of $I_S$, is subtracted from $I'_R$, an attenuated form of the reference current ($I_R$); the result is supplied to a transimpedance amplifier. The output of the amplifier, $V_C$, controls the current injection block. When $I_S < I_R$, this block absorbs an extra current, $I_J$, and maintains $I_S$ close to $I_R$.

Fig. 2 shows the schematic representation of the proposed circuit. The rationale behind each individual block, as well as the

* Corresponding author. Tel.: +1 905 593 8697.
*E-mail addresses:* hvahedi@uoguelph.ca (H. Vahedi), sgregori@uoguelph.ca (S. Gregori), rmuresan@uoguelph.ca (R. Muresan).

0026-2692/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.mejo.2010.08.011

specific considerations, which guarantee the desired functionality will be explained in the following subsections.

### 2.1. Current sensor

The current sensor is a modified current mirror (transistors M1 and M2 along with the differential amplifier M21–M25). The current mirror is a reliable and highly sensitive circuit since the mirroring ratio of the current depends exclusively on the transistors' ratio. However, there is a drawback: the insertion of the current mirroring transistor (M1) in the supply line adds a voltage drop equal to the $|V_{GS}|$ of M1. To remedy this problem, a feedback loop has been created, using a differential amplifier, to maintain a constant small voltage drop across M1. The differential amplifier, consisting of transistors M21–M25, compares the supply voltage of the microcontroller with a reference voltage $V_{ref}$. This loop has two more benefits:

(1) it guarantees that M1 remains in saturation region and the current sensor functions properly for all current values;
(2) M1 in saturation region decouples the global supply line ($V_{DD}$) and the supply pin of the microcontroller ($V_{DD-C}$) and does not allow ripples of the global supply voltage to affect the operation of the microcontroller.

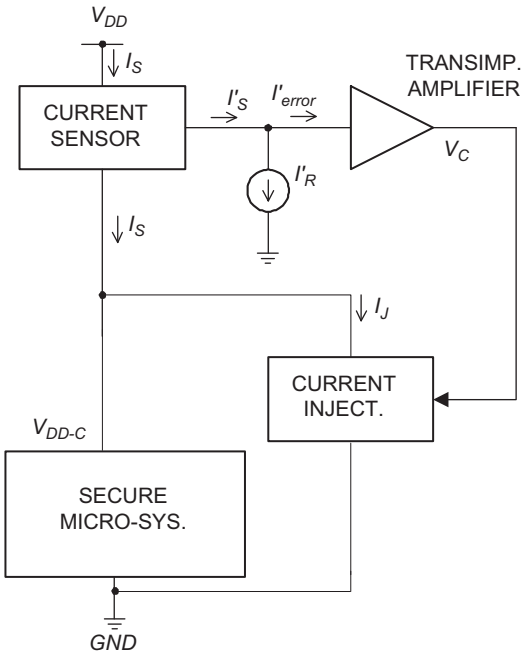


**Fig. 1.** Block diagram of the proposed circuit.

In designing the current sensor, the goal was to keep the voltage drop across the current sensor as low as possible. To that end, the reference voltage of the differential amplifier and the sizes of the mirror transistors (M1 and M2 in Fig. 2) were chosen, so that these two transistors are kept at the lower end of the saturation region. Hence, the voltage drop across the mirroring transistor (M1) is small (250 mV, i.e., 15% of the power supply), while the transistors replicate the current with a reasonable precision.

### 2.2. Transimpedance amplifier

The current $I'_{error}$ is injected into the transimpedance amplifier (transistors M8–M16) [11]. $I'_{error}$, the current entering the common source of M8 and M9 (i.e., the low-impedance node $S$), is split with a ratio of $g_{m8}/g_{m9}$. The resultant currents are mirrored, amplified, and converted into the voltage $V_C$ by passing through current mirrors (M10 and M12) and (M11 and M13). $V_B$ is the bias voltage and is provided by a current mirror configuration. The relationship between the input and the output of the amplifier is:

$$V_C = \frac{(W/L)_{12}}{(W/L)_{10}} R_{V_C} I'_{error} \tag{1}$$

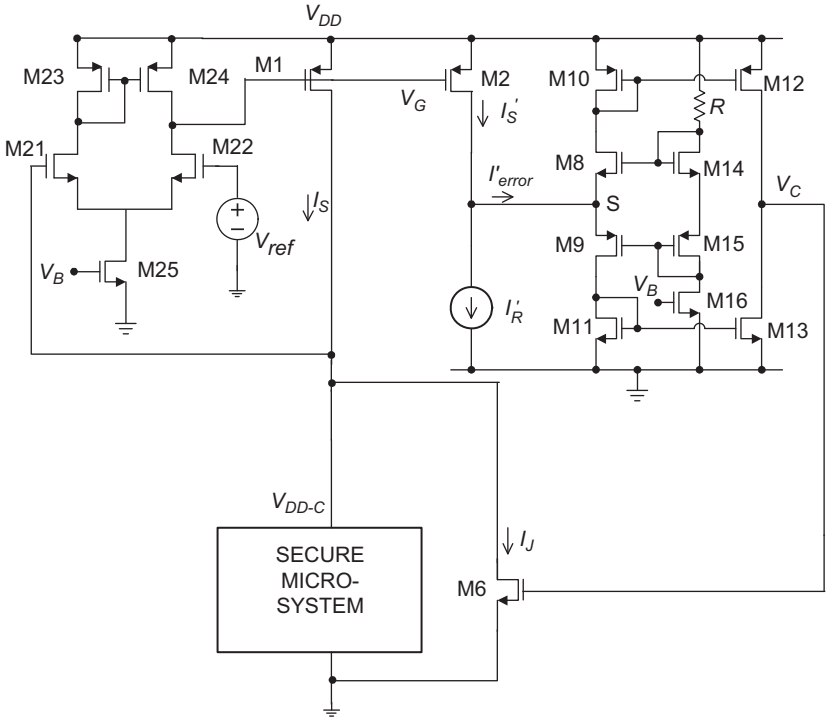


**Fig. 2.** Current flattening circuit schematic representation.