Proceedings of the 10th WSEAS International Conference on CIRCUITS, Vouliagmeni, Athens, Greece, July 10-12, 2006 (pp81-84)

Role of Parasitic Capacitors of MOS Transistors in Cryptographers

MOHSEN HAYATI - SEYED MOHSEN YAGHOUBI
Electrical Engineering Department
Islamic Azad University-Kermanshah Branch
Kermanshah
IRAN

Abstract: This paper describes the parasitic capacitors of MOS transistors and their important role in constructing a clear power consumption pattern of devices built on this technology. But the sensitivity of power consumption pattern to parasitic capacitor makes the cryptographer vulnerable to attacks. We are going to describe this dependency and make the cryptographer more secure.

Key Words: MOS, Power Analysis, Smart Cards, Inverter, Cryptograph.

1 Introduction

Smart cards have provided so many facilities that nowadays cards are capable to serve in several situations. They can be used in e-commerce, access control issues, credit cards, electronic passport, storing private and sensitive data and many other fields. Securing information stored on smart cards is one of the most important concerns to smart card developer companies. So they reap the benefits of several security tasks. Cryptographic devices encrypt data in order to make them vague for unauthorized access attempts [1]. These devices are made of MOS transistors. Due to parasitic capacitors of these transistors, power consumption pattern will reveal important information about the instructions running. Differential Power Analysis (DPA) is on of the most strong and efficient approaches to obtain a clear pattern of power consumption in electronic devices [2-3].

2 Preventing Differential Power Analysis

Techniques for preventing differential power analysis and related attacks fall roughly into three categories[4-7]. A first approach is to reduce signal sizes,such as by using constant execution path code,choosing operations that leak less information in their power consumption,balancing Hamming weights and state transitions,and by physically shielding the device.Unfortunately such signal size reduction generally can not reduce the signal size to zero,as an attacker wiyh an infinite number of samples will still be able to perform differential power analysis on the signal.

A second approach involves introducing noise into power consumption measurement.Like signal size reductions,adding noise increases the number of samples required for an attack,possibly to an infeasibly large number.In addition,execution time and order can be randomized. Designer and reviewers must approach temporal obfuscation with greater caution,however,as many techniques can be used to bypass or compensate for these effects.Several vulnerable products have passed reviews that used data processing methods.For safety it should be possible to disable temporal obfuscation methos during review and certification testing.

A final approach involves designing cryptosystems with realistic assumptions about the underlying hardware.Nonlinear key update procedures can be employed to ensure that power traces cannot be correlated between transactions.

3 Preventing Simple Power Analysis

Techniques for preventing simple power analysis[6-9] are generally fairly simple to implement,Avoiding procedures that use secret intermediates or keys for conditional branching operations will mask many simple power analysis characteristics. In cases such as algorithms that inherently assume branching,this can require creative coding and incur a serious performance penalty.Also,the microcode in some microprocessors cause large operand-dependent power consumption features.For,these system,even constant execution path code can have serious

simple power analysis vulnerabilities.Most hard-wired hardware implementations of symmetric cryptographic algorithms have sufficiently small power consumption variations that simple p[ower analysis does not yield ker material.

4 Parasitic Capacitors

In Fig.1 you can see the parasitic capacitances of MOS transistor [8].

4.1 Input capacitors

Input capacitors are consisting of three main parts
1.Gate capacitance
2.Diffusion capacitance
3.Routing capacitance

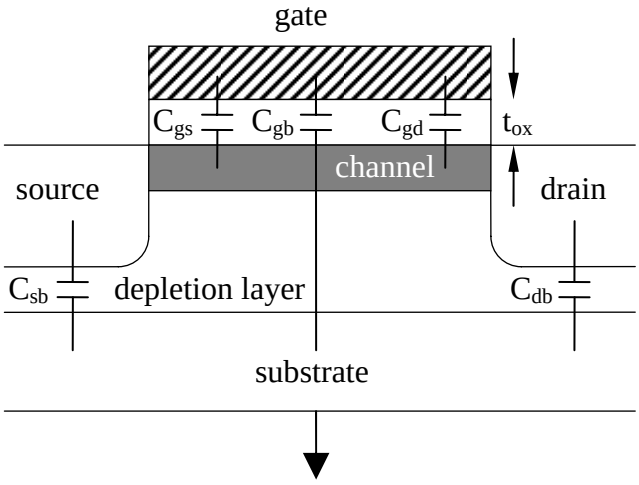

Fig.1- MOS parasitic capacitances.

As we know, the capacitance of silicon oxide in Fig.1 is given by [1],

$$C_0 = \left(\frac{\varepsilon_0 \varepsilon_{SiO_2}}{t_{ox}} \right) A$$

$A =$ Area of gate

And the capacitance of depletion layer is,

$$C_{dep} = \left(\frac{\varepsilon_0 \varepsilon_{Si}}{d} \right) A$$

$d =$ Depletion layer depth

$\varepsilon_{Si} =$ Dielectric constant of silicon = 12

So Gate-Bulk total capacitance will be [1],

$$C_{gb} = \frac{C_0 C_{dep}}{C_0 + C_{dep}}$$

Referring to Fig.1,the total capacitance of Gate is,

$$C_g = C_{gb} + C_{gs} + C_{gd}$$

Because the input signal of a cryptographer is a clock pulse, we have transistors in two main regions of OFF and saturation. In OFF region the gate source voltage is below threshold voltage, so we have no channel to conducting carriers, hence we have

$$C_{gs} = C_{gd} = 0$$

And

$$C_{gb} = \frac{C_0 C_{dep}}{C_0 + C_{dep}}$$

In saturation region, where $V_{gs} - V_t < V_{ds}$ and the channel is heavily inverted. The drain region of the channel is pinched off. So we have

$$C_{gd} \to 0$$

$$C_{gs} \to \frac{2}{3}\left(\frac{\varepsilon_0 \varepsilon_{SiO_2}}{t_{ox}} \right) A$$

And

$$C_{gb} \to 0$$

4.2 Diffusion Capacitance

Diffusion capacitors are consisting of area capacitors and peripheral capacitors.

$$C_d = C_{ja}(ab) + C_{jp}(2a + 2b)$$

Where:

$C_a =$ Area Capacitance

$C_p =$ peripheral capacitance

Typical values of area and peripheral capacitors for n-Device are

$$C_{ja} \approx 3 \times 10^{-4} \frac{\text{pf}}{\mu\text{m}^2}$$

$$C_{jp} \approx 4 \times 10^{-4} \frac{\text{pf}}{\mu\text{m}}$$

5 Cryptographers

Cryptography is a procedure that is used to increasing Data security when it is stored in a memory to avoid unauthorized access to it or when it is transferred from a source to a destination.[9] For example when a smart card is transacting with a terminal or a smart card reader. Cryptographic algorithms use these principles for encoding data:

1.Mathematical and logical calculations
2.Shifting and rotating
3.Look up tables
4.Access to registers
These calculations are vulnerable to power analysis algorithms such as SPA and DPA. These algorithms can estimate the output power consumption and compare it with the patterns that previously obtained via applying basic inputs. So they can guess the sequence of instructions and in this way the content of EEPROM or ROM of a smart card can be identified for an invalid person.
Cryptographers usually use basic circuits for encoding data. One of these basic circuits is Inverter that is shown in Fig.2 [10].

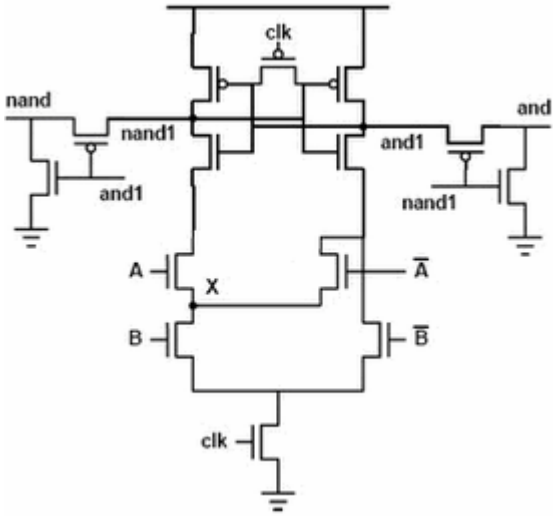

Fig.2- Inverter with AND NAND output.

We should keep in mind that for showing the logic of 0 or 1, we consider the charging or discharging of a capacitor in the output of the circuits. The problem is, when the capacitance of parasitic capacitors is relatively high, then it is possible that the logical values of internal nodes remains floated i.e. between logic 0 and 1. Furthermore, sub threshold currents exist in transistors that have two conditions as below
1.Vgs<Vt
2.Vds>0

This means that apparently OFF transistors that have Vds>0, can cause to float the internal nodes. The response of the circuit of Fig.2 is shown in Fig.3.

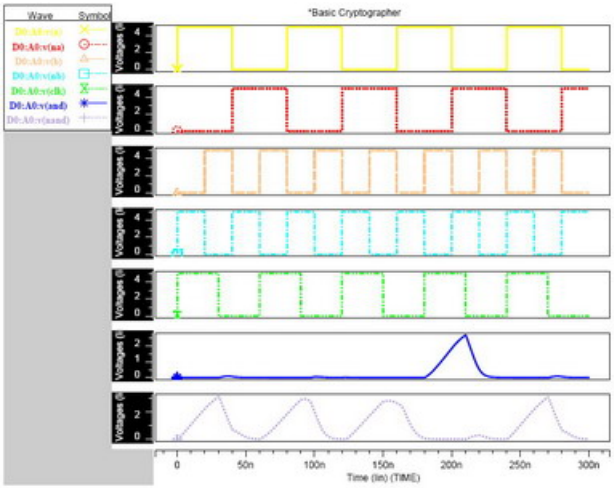

Fig.3-The response of a Basic Inverter.

When transistor M1 is added to Inverter as shown in Fig.4, we can see the improved response that outputs doesn't cross noise margin region. This is due to the fact that M1 provide the discharging path for internal nodes in the mode of evaluation of the inverter.

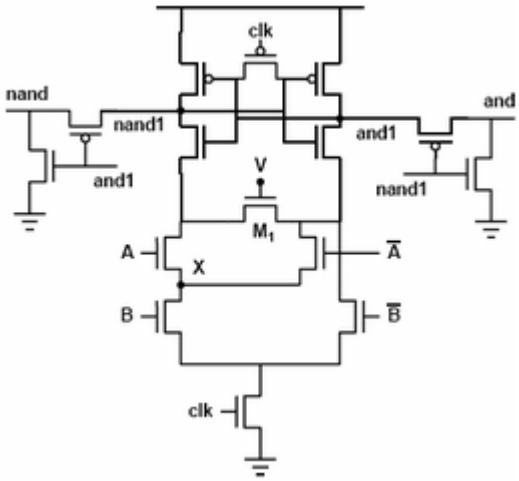

Fig.4- Modified Inverter (Corrected Inverter).

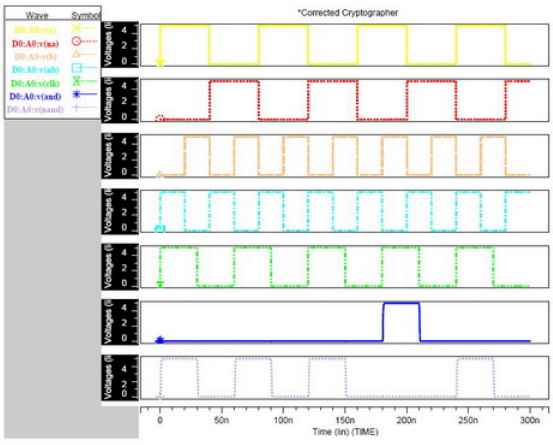

Fig.5- Response of modified inverter.

The improved response of modified inverter is shown in Fig.5.

6 conclusions

The inverter is more symmetric and it doesn't give good information about power consumption of itself.

In the inverter circuit, we have to take more non ideal assumptions, where one of them is that the path of inputs to corresponding outputs doesn't have the same equivalent capacitance. Furthermore the transistors are not completely the same (similar).

References:

[1]W.RANKL,W.EFFING, Smart Card Handbook, Giesecke & Devrient.Gmbh Munich, Germany,John Wiley &Sons .Ltd,2000

[2]U.Neffe ,K.Rothbart, Ch.Steger, R.Weiss , E.Rieger , A. Muhlberger Energy Estimation Based on Hierarchical Bus Models for Power-Aware Smart Cards , Graz University of Technology & Philips Semiconductors BL Identification.

[3]Harold.F.Tipton , Micki Krause ,CISSP, Information Security Management Handbook 2004 by CRC Press.

[4]P. Kocher,J. Jaffe and B.Jun,Differential power analysis,Cryptography research ,Inc.,San Francisco,CA 94105,USA.

[5]E.Biham and A.Shamir, Differential cryptanalysis of the data encryption standard,Springer-Verlag,1993.

[6]D. Boneh,R. Demillo and R. Lipton,On the importance of checking cryptographic protocols for faults,Advances in cryptology,Proceeding of EURO-CRYPT ,97, Springer-Verlag, May 1997,pp. 35-51.

[7]M.Matsui,The first experimental cryptanalysis of the data encryption standard,Avances in cryptology ,Proceeding of Crypto, 94 ,Springer-Verlag,August 1994,pp. 1-11.

[8]Neil H.E.Weste, Kamran Eshraghian, ADDISON-WESLEY, 1992.pp 180-188.

[9]Donal O'Mahony , Michael Peirce ,Hitesh Tewari , Electronic Payment Systems foe E-Commerce Second Edition.

[10]Kris Tiri and Ingrid Werbauwhede, Charge Recycling Sense Amplifier Based Logic, Electrical Engineering Department,UCLA.