Exploiting Semiconductor Properties for Hardware Trojans

Y. Shiyanovskii, F. Wolff, C. Papachristou
Case Western Reserve University
Cleveland, Ohio 44106, USA
{yxs32, fxw12, cap2}@case.edu

D. Weyer, W. Clay
Rockwell Automation
{djweyer,sclay}@ra.rockwell.com

Abstract. This paper discusses the possible introduction of hidden reliability defects during CMOS foundry fabrication processes that may lead to accelerated wearout of the devices. These hidden defects or hardware Trojans can be created by deviation from foundry design rules and processing parameters. The Trojans are produced by exploiting time-based wearing mechanisms (HCI, NBTI, TDDB and EM) and/or condition-based triggers (ESD, Latchup and Softerror). This class of latent damage is difficult to test due to its gradual degradation nature. The paper describes life-time expectancy results for various Trojan induced scenarios. Semiconductor properties, processing and design parameters critical for device reliability and Trojan creation are discussed.

I. Introduction

Due to the high capital costs of building and maintaining fabrication facilities, the number of fabs is shrinking. Hence, there has been a major shift in control over the fabrication process for integrated circuits (IC). More and more vendors outsource the fabrication process to off shore fabrication facilities [1]. Using such facilities makes the integrated circuits vulnerable to malicious alterations. These alterations are more commonly known as hardware trojans and are usually created by insertion of additional logic circuitry [1]. The intent of these trojans ranges from functional changes of the circuit to a complete system failure. Testing for Trojans at the manufacturing level have been investigated using power analysis techniques [2], [3], [4], delay testing [5], and using test vectors [6].

In this paper we describe a new type of Trojan that can be induced by intentional modification of fabrication process to accelerate wearing processes in CMOS devices. These process modifications can keep the initial performance parameters of the integrated circuit within the accepted variation. Such Trojans can exploit the following wearing processes: Hot Carrier Injection (HCI), Oxide Breakdown (OB), Negative Bias Temperature Instability (NBTI), Electron Migration (EM).

IC manufactures optimize their processes to ensure the effects of the time based wear out mechanisms to guarantee the lifetime of a device for 10 plus years over a specific temperature range i.e. 0 to 70 °C for commercial devices. IC manufactures bound their process control limits to ensure production devices will not be affected by the time based wear out mechanisms for the guaranteed lifetime of the device. Figure 1 shows the normal distribution of the manufacturing process with the probability of a time based defect occurring within the guaranteed device lifetime.

Production tests are not performed for these effects as they are time based, and the testing costs would be prohibitive. The production tests are optimized to find defects using the lowest cost equipment in minimal test time, and an acceptable test coverage to guarantee the devices are functional. The time based effects can be accelerated, but the test times are in days, which is not practical for production.

A process engineer could maliciously modify certain steps in the process that would cause some or all devices on a wafer to wear out in months to few years, thus creating a reliability based Trojan. The paper will expound on process modifications that could be maliciously used to create reliability based Trojans. Figure 1 illustrates how the process engineer could modify a step in the manufacturing process to increase the probability that devices will be produced with a time based wear out mechanism. The parameters that affect these mechanisms are exponential in nature, so only small changes are needed in process steps. The overlap area in Figure 1 illustrates that a certain percentage of the devices on the wafer will be infected with these reliability Trojans.

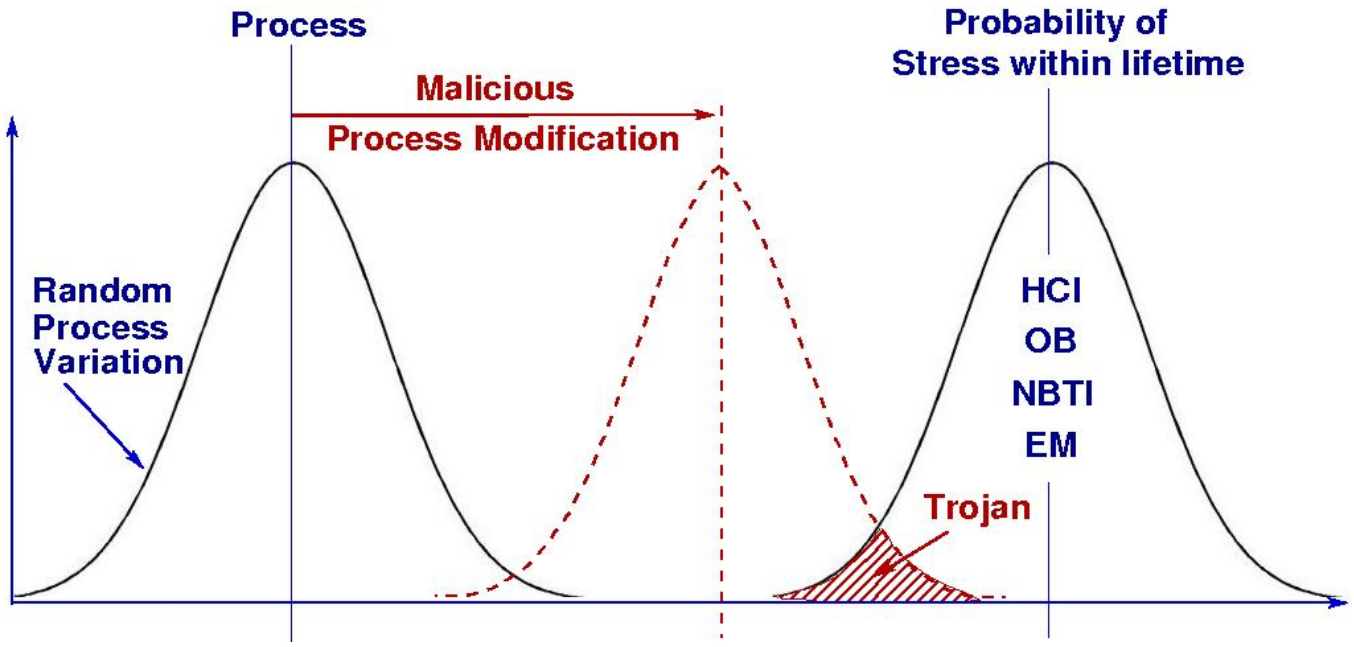

Fig. 1. Shifting the Process Variation to induce a Hardware Trojan based on Stress

II. Wearing Mechanism of CMOS Devices

In this section, we discuss the following wearing processes in CMOS devices. Hot Carrier Injection (HCI), Oxide Breakdown (OB), Negative Bias Temperature Instability (NBTI), Electron Migration (EM) We explore different degradation models and lifetime models for each process to identify critical dependencies that can be exploited via a Trojan device by process characterization manipulation.

A. Hot Carrier Injection:

The term hot carrier injection describes electrons (holes) that have accumulated sufficient kinetic energy to overcome potential barrier and be injected into the gate oxide. Such accumulation becomes more prominent in high electric field for electrons that have avoided subsequent scatterings with the lattice atoms. The carriers must overcome the $Si - SiO_2$ energy barrier of about $3.7eV$ for electrons and $4.6eV$ for holes. For NMOS, hot electrons are produced and for PMOS holes are produced.

Injection of hot carriers can result in the following: generation of new traps at or near the $Si - SiO_2$ interface or generation of new traps in the oxide itself. The traps located at $Si - SiO_2$ interface affect the transconductance, g_m, and leakage current of the device. The traps that are located in the gate oxide increase the threshold voltage, V_{th}. The carriers can also increase the substrate current, I_{sub}. Thus, the HCI degradation can be monitored through shifts in the threshold voltage or transconductance and drain current.

There are different models for predicting the lifetime of the device based on the rate of HCI effect. One of such models uses a relationship between the shifts in gate current, I_{gate}, and the HCI degradation, [7]. The model assumes that the rate of HCI damage to the CMOS device, Δ, is proportional to the gate current, I_{gate}, and can be expressed by the following equation:

$$\Delta/dt \sim I_{gate} = \frac{A(\Delta)}{W I_{drain}} * (\frac{I_{sub}}{I_{drain}})^m, \qquad (1)$$

where W is the width of the CMOS device, [8], [7]. Abbreviating the following, $B = A(\Delta)/W$ and merging that Median Time To Failure depends on the reciprocal of $d\Delta/dt$, the failure rate is found from

$$\lambda = B I_{drain} (\frac{I_{sub}}{I_{drain}})^m \qquad (2)$$

The following equation assumes static voltages and currents, in order to determine dynamic degradation, λ must be integrated over a full cycle time, [7] Such model also does not include the effect of operational temperature on the lifetime of the device. However, the temperature does influence the rate of the HCI degradation and must be modeled accordingly. In order to include temperature in the MTTF, the model must be

based on the changes in substrate current. The MTTF equation is the following:

$$MTTF_{HCI} = B(I_{sub}) - N\exp(\frac{E_a}{kT}), \quad (3)$$

where B is a scale factor which is a function of doping profiles, sidewall spacings and dimensions that are specific to the manufacturing process characterization (I_{sub}) is the substrate current, N ranges from 2 to 4,k for the Boltzmann's constant, T is temperature, and E_a is the activation energy in the range of $-0.1eVto-0.2eV$.

There is another way to model HCI degradation, through a power law dependence on the stress time, t. The HCI effect can be seen in shifts for the threshold voltage V_{th} due to increased trap generation in the oxide and the interface. Wang [9] proposed the following model for the rate of change for the threshold voltage V_{th} for NMOS devices:

$$\Delta V_{th} \sim \sqrt{Q_i}\exp(\frac{E_{ox}}{E_o})\exp(-\frac{\phi_{it}}{q\lambda E_m})t^{n'}, \quad (4)$$

where E_{ox} is the oxide electric field, E_m is the lateral electric field, Q_i is the inversion charge, ϕ_{it} is the trap generation energy, λ is the hot electron mean free path and E_o is the process-dependent factor. The model does not include the temperature (T) factor or the width (W) factor as seen in the $Equation(3)$ and $Equation(1)$ respectively.

B. Oxide/Dielectric Breakdown (OB):

In CMOS devices the strong electric fields across the gate oxide can cause some material damage that will lead to formation of a conductive path. The conductive path within the dielectric will create a short between the substrate and the gate, thus nullifying the isolating properties of the gate oxide and resulting in complete oxide failure. The oxide breakdown is a rather local phenomenon in which holes and bulk electron trapping damage the oxide material. There are two types of oxide breakdown: early life oxide breakdown and time-dependent dielectric breakdown.

The early life oxide breakdown is created through impurities and weak chains within the dielectric layer which is a direct result of the manufacturing process. Any heavy alteration within the manufacturing process that will greatly increase trap generation within the oxide will lead to early oxide breakdown. Increase in trap generation can be caused by the following factors: presence of mobile sodium (Na) ions in the oxide, impurities trapped on the silicon interface during the oxidation, and crystalline defects in the silicon. Time-dependent dielectric breakdown (TDDB) consists of two phases: a build-up phase and a runaway phase,[7]. During the build-up phase, bulk electrons and holes gets randomly trapped through out the oxide. The number of traps increase with time, forming a high electric field which depends on the voltage and oxide thickness[10].

$$E_{ox} = \frac{V}{d_{ox}} \quad (5)$$

Once the trap density reached the critical trap density the runaway phase begins. During the runaway phase, the total electric field produced by the trapped electrons and holes exceeds the dielectric breakdown threshold,[10]. Once the electric field is strong enough, a conducting path is formed within the oxide and current begins to flow between the substrate and the gate. Due to this behavior the time to total device failure due to oxide breakdown can be modeled using Weibull probability distribution.

The rate of trap generation is the key component in determining the rate of oxide degradation and breakdown. There are three general models for trap generation in the oxide: Anode Hole Injection (AHI) model, Thermo-Chemical (TC) model and Anode Hydrogen Release (AHR) model, [7] These models are contradictory in their explanation of the trap generation and the acceleration in the law of time-to-breakdown - t_{BD}. However two of the models, AHI (E model) and TC (1/E model) can be summarized as follows:

$$t_{BD} = \tau_0 * \exp(-n * \gamma * E_{ox}^n) \quad (6)$$

where τ_0 and γ are constants and n is either 1 for (E model) or -1 for ($\frac{1}{E}$ model). Both of these models are designed primarily for thick gate oxides.

For ultra-thin oxides the primary driver of the breakdown process is gate voltage and at higher temperatures the process is accelerated even more. To account for these factors, a new relationship has been proposed for the Median Time To Failure (MTTF) for the oxide breakdown:

$$MTTF_{OB} = T_{BD0}(V)\exp(\frac{a(V)}{T} + \frac{b(V)}{T^2}), \quad (7)$$

where T_{BD0}, a and b are voltage dependent factors and $\frac{b}{T^2}$ accounts for the temperature effect. There is another MTTF model for thin oxides:

$$MTTF_{OB} = A\exp(\frac{B}{E_{ox}})\exp(\frac{Ea}{kT}), \quad (8)$$

where B stands for the electric field acceleration factor, k for the Boltzmann's constant, and T for the absolute temperature.

C. Electromigration:

The electromigration (EM) effect can play a critical role in circuit reliability at high current density (typically exceeding 10^5 A/cm^2),[7]. Energy and momentum from electrons can be transferred to metal atoms and lead to their biased movement towards the anode electrode. This mass transport through interface diffusion or grain boundary diffusion will create material depleted regions near the cathode and regions with access material near the anode. As a result, the layer could be damaged and the damage is manifested as open circuit failure near the cathode or short circuit failure near the anode regions. EM is a thermally activated process and the median time to failure (MTTF) can be described by the simplified formula

$$MTTF_{EM} = A * (j_e)^{-n} \exp(\frac{E_a}{kT}) \tag{9}$$

where E_a is the activation energy of EM process, j_e is the current density, A is a fabrication-dependent constant and n can vary from $1 < n < 2$ depending on metal properties,[7],[10]. Both the activation energy E_a and A constant depend on fabrication technology and are defined by material type, grain structure, size distribution, crystallographic orientation and impurities. The constant A also depends on the geometry and length of interconnects. It was shown, that activation energy can be reduced more than twice (from $1.4eV - to - [0.5 - 0.8]eV$) by doping Al with a small amount of Cu (0.3-5%), [7]. In reality, the EM failure is a complicated process and non-Arrhenius temperature effects should be taken into consideration to predict the failure times.

The poor metal quality, vacancies, and multiple irregular grain boundaries result in significant reduction of the activation energy that has severe effect on the median time to failure due to an exponential dependence. Electromigration induces stress gradients that compete with EM mass transfer by causing ion movement from compressive stress regions to regions with tensile stress.

Material type and methods of interconnect deposition for submicron SMOC technologies (physical vapor deposition, PVD chemical vapor deposition, CVD; atomic layer deposition, ALD; electroplating; annealing; chemical-mechanical or electro-chemical-polishing) play critical role in grain microstructure of interconnects that determines the mass transport path and EM lifetimes.

D. Negative bias temperature instability

Negative Bias Temperature Instability (NBTI) is known since the very early developments of MOS devices; however, it is emerging as one of the major degradation mechanisms for deep-submicron CMOS technologies. NBTI causes a significant threshold voltage shift $(50 - 100mV)$ and decrease in drain current mostly in p-channel metal-oxide-semiconductor field effect transistors (pMOSFET) under a negative gate bias at elevated temperatures $(100 - 150°\mathrm{C})$. The effect is due to creation of interface traps and to buildup of positive oxide charge over periods of time (from several months to years depending on the device operation conditions). Trapped holes can be thermally activated and can cause dissociation of oxide defects. The threshold voltage shift ΔV_{th} is expressed as:

$$\Delta V_{th} = A(V_g, t) \exp(-E_{NB}/kT) \tag{10}$$

where E_{NB} is the NBTI activation energy and $A(V_g, t)$ is a function of gate voltage and time,[7],[11],[10].

There are many models proposed to explain the NBTI effect, including oxide hole injection, electron tunneling and diffusion-reaction models. The most accepted model is the diffusion-reaction (or electrochemical) concept that relates the activation energy E_{NB} to diffusion of hydrogen species dissociate at the interface with multiple hydrogen-terminated Si bonds $(Si - H)$.

Deposition processes for current MOSFETs employ oxynitride, $SiON$ layer as a gate dielectric material deposited by plasma enhanced CVD or rapid thermal oxidation in presence of NO or NO_2 gases. It was shown that while introduction of nitrogen into oxide layer improves transistor performance and increases dielectric constant of gate material, it also reduces NBTI lifetime by introducing bulk oxide defects and reducing thermal activation energy of defect generation at $Si/SiON$ interface. The threshold voltage shift and NBTI lifetime strongly depend on the interfacial nitrogen concentration at the SiO_2/Si interface that can be controlled by temperature, pressure, duration of the thermal nitridation processing step. Typical range of the nitrogen concentration is around 2-15% for the thermal nitridation process. Higher interfacial N concentrations are usually achieved using decoupled plasma nitridation. The higher nitrogen concentration, the larger ΔV_{th} shift during NBTI stress.

TABLE I
SEMICONDUCTOR PROPERTIES

Degradation Mechanisms	Lifetime Equation	Failure	Factors that effects critical parameters
Hot Carrier Injection (HCI)	$MTTF_{HCI} = B(I_{sub}) - N\exp(\frac{E_a}{kT})$	1) **critical** device switching time delay 2) **non-responsive** device functionality	1) Drain doping levels 2) Channel lengths 3) Gate oxide thickness 4) Interface traps 5) Purity and quality of gate oxide
Oxide Breakdown (OB)	$MTTF_{OB} = A\exp(\frac{B}{E_{ox}})\exp(\frac{Ea}{kT})$	1) **short circuit** between the gate and the substrate	1) Purity of oxide layer a) Crystal defects b) Impurities (e.g., heavy metals) c) Roughness of oxide surface 2) Gate oxide thickness
Electromigration (EM)	$MTTF_{EM} = A * (j_e)^{-n}\exp(\frac{E_a}{kT})$	1) **short circuit** conditions 2) **open circuit** conditions	1) Interconnect metal type 2) Grain structure 3) Grain size distribution 4) Crystallographic orientation 5) Impurities 6) Geometry and length of interconnects
Negative bias temperature instability (NBTI)	$\Delta V_{th} = A(V_g, t)\exp(-\frac{E_{NB}}{kT})$	1) **critical** device switching time delay 2) **non-responsive** device functionality	1) Nitrogen concentration near Si/SiO2 interface, 2) Presence of boron 3) Water near Si/SiO2 interface 4) Gate dimensions 5) Gate oxide thickness

III. CRITICAL PROCESS PARAMETERS

In this section, the critical process factors, that yield maximum results for exploiting the wearing effects described in the previous sections, are investigated. The exponential nature of lifetime prediction of the device for the wearing effects gives rise to Trojan alterations that greatly accelerate the wearing mechanics of the device.

Table I shows a list of factors that can be modified during the process manufacturing to induce reliability Trojans through the time-based wearing effects. The table shows the degradation mechanism, the lifetime prediction model, the critical failures resulting from the degradation mechanism, and the critical factors.

Knowing the process model, a process engineer can influence one or more steps in the IC fabrication to change one or more critical factors. This change will inherently result in an accelerated MTTF model for one or more degradation mechanism. The malicious process modification (reliability Trojan) will guarantee higher probability of the devices produced will have a greatly reduced lifetime, as shown in Fig. 1.

IV. FUTURE WORK

The process modifications of time based wear out mechanisms of HCI, NBTI, OB and EM will be simulated using TCAD to illustrate how variation in the IC process, effect device lifetimes. We will show how these wear out mechanism could be exploited for Trojans by design modifications. We will also introduce condition-based trigger class of Trojans, by investigating how the phenomena of ESD, Latchup and soft errors could be

exploited as Trojans. We will illustrate how packaging modifications could also be used to maliciously create Trojans.

V. Conclusion

This paper discussed the concept of a new class of hardware Trojan that exploits early wear out mechanisms in CMOS devices. There are no detection techniques that can detect all the variations of these reliability based Trojans. In any post-production tests the infected transistor are operating just as well as normal transistors with no discrepancy in performance. The danger lies in the fact that until the Trojan transistor has been in operation for some time, the circuit appears as if no malicious alterations have been inserted. These reliability Trojans are induced through minor variations in the manufacturing process. Thus, there is a critical demand for detection techniques that properly identify these Trojans.

References

[1] S. Adee, "The hunt for the kill switch," *IEEE Spectrum*, pp. 34–39, May 2008.

[2] Y. Jin and Y. Makris, "Hardware trojan detection using path delay fingerprint," *IEEE Intl. Workshop on Hardware-Oriented Security and Trust (HOST'08)*, pp. 51–57, 2008.

[3] R. Rad, J. Plusquellic, and M. Tehranipoor, "Sensitivity analysis to hardware trojans using power supply transient signals," *IEEE Intl. Workshop on Hardware-Oriented Security and Trust (HOST'08*, pp. 3–7, 2008.

[4] M. Banga and M. Hsiao, "A region based approach for the identification of hardware trojans," *IEEE Intl. Workshop on Hardware-Oriented Security and Trust (HOST'08)*, pp. 40–47, 2008.

[5] J. Li and J. Lach, "At-speed delay characterization for ic authentication and trojan horse detection," *IEEE Intl. Workshop on Hardware-Oriented Security and Trust (HOST'08)*, pp. 8–14, 2008.

[6] X. Wang, M. Tehranipoord, and J. Plusquellic, "Detecting malicious inclusions in secure hardware: Challenges and solutions," *IEEE Intl. Workshop on Hardware-Oriented Security and Trust (HOST'08)*, pp. 15–19, 2008.

[7] J. Bernstein, M. Gurfinkel, X. Li, J. Walters, Y. Shapira, and M. Talmor, "Electronic circuit reliability modeling," *Microelectronics Reliability*, pp. 1957–1979, 2006.

[8] W. Wang, "Dependence of hci mechanism on temperature for 0.18 micron technology and beyond," *Integrated Reliability Workshop Final Report*, 1999.

[9] ——, "Compact modeling and simulation of circuit reliability for 65nm cmos technology," *Measurement*, 2007.

[10] G. Gielen, P. De Wit, J. Martin-Martinez, B. Kaczer, and G. Groeseneken, "Emerging yield and reliability challenges in nanometer cmos technologies," *Design, Automation, and Test in Europe (DATE'08)*, 2008.

[11] J. Stathis and S. Zafar, "The negative bias temperature instability in mos devices," *Microelectronics Reliability*, 2006.