AQFP Performance In Detection Of Recycled ICs Based On RO And AF Sensors

K. Padmapriya
M.E - Communication System, Dept of ECE, PREC, Thanjavur, Tamilnadu, India

R. Ramya
Assistant Professor, Dept of ECE, PREC, Thanjavur, Tamilnadu, India

Abstract: Counterfeiting and recycling of integrated circuits (ICs) have become major issues. It would be extremely difficult to distinguish recycled ICs from unused ICs. Used IC can act as a ticking time bomb and it is used for much critical application. An adversary can include additional die on top of the recycled die carrying a back-door attacker based and AF based sensors are used to identify the recycled ICs. Develop on chip sensors to detect analog ICs. Along with this operation we include the AQFP (adiabatic quantum-flux-parametric) to reduce the power leakage and store the power in Latches and used for next Operation. Therefore, it is vital that we prevent these recycled ICs from entering critical infrastructures, aerospace, medical, and defense supply chains.

Keywords: Ring oscillator, Antifuse sensor, Antifuse memory, Recycling IC’s

I. INTRODUCTION

Recycling of ICs have become major issues in recent years. It potentially impacts the security and reliability of electronic systems bound for military, financial, or other critical applications. With identical functionality and packaging, it would be extremely difficult to distinguish recycled ICs from unused ICs. These components are then sold as new in the open market. In some cases, the recycled parts may either be nonfunctioning, not performing to manufacturer specifications, or the prior usage has done significant damage to the part’s life cycle and introduces major reliability concerns. In some cases, new parts have also been remarked by counterfeiters. The remarked parts may be equivalent part types from a cheaper brand or new parts are remarked to a higher grade.

As the recycling process usually involves a high-temperature environment to remove ICs from boards, there are several security issues associated with these ICs such as: a used IC can act as a ticking time bomb as it does not meet the specification of the unused ICs. Therefore, it is vital that we prevent these recycled ICs from entering critical infrastructures, aerospace, medical, and defense supply chains. In general, the recycled ICs have the original appearance, functionality, and markings as the devices they are meant to mimic, but they are used for a period before they are resold. Even the best visual inspection techniques will have difficulty in identifying these ICs with certainty. Additionally, because recycled ICs contain the original correct die internally, decamping technologies will provide little assistance in their detection. It is important to develop new techniques to help in measuring these ICs’ specifications and effectively detect them if they are already used even for a short period.

The counterfeiting of electronic components has become a major challenge in the 21st century. The electronic component supply chain has been greatly affected by widespread counterfeit incidents. A specialized service of testing, detection, and avoidance must be created to tackle the worldwide outbreak of counterfeit integrated circuits (ICs). So far, there are standards and programs in place for outlining the testing, documenting, and reporting procedures. However, there is not yet enough research addressing the detection and avoidance of such counterfeit parts. In this paper we will present, in detail, all types of counterfeits, the defects present in them, and their detection methods. We will then describe the challenges to implementing these test methods and to their effectiveness. We will present several anti-counterfeit measures to prevent this widespread counterfeiting, and we also consider the effectiveness and limitations of these anti-counterfeiting techniques.

The vast majority of counterfeits is “recycled” components that have been crudely reprocessed (often washed...
in a river) and re-marked. The most dangerous are ones that still function electrically but have unpredictably short lifespan. More than 360,000 counterfeit integrated circuits (ICs) have been seized by U.S. and European customs. It’s the millions that make it through undetected that are worrisome. When one of these fake, unreliable or faulty ICs fails in a critical application such as an aerospace, military or healthcare application, the consequence can be a matter of life and death. Even in less critical applications, faulty components can wreak havoc.

![Fake IC](image)

**Figure 1: Fake IC**

**A. COUNTERFEIT ICS: A GROWING THREAT**

Some counterfeit integrated circuits are pure “fakes” stamped with reputable brand identification. In the most egregious cases, fakes can be empty shells without internal circuitry. More commonly however, counterfeit ICs are previously used and recycled brand name ICs. After usually uncontrolled removal from their PC boards, they are cleaned up, “repainted” (blacktopped) and printed with new serial numbers and date codes. They can even be shipped in authentic carriers and reels (previously used). The counterfeits may be visually indistinguishable from authentic ICs; their fresh exterior masks hidden flaws and defects. Recycled counterfeit ICs cannot always be identified with basic electrical tests or external visual inspection.

**II. ANTICIPATED WORK**

**A. AF (ANTIFUSE SENSOR)**

ADC can used to convert the analog input in to a lower clock frequency signal; Counter is used to measure the cycle count of the lower frequency signal. The size of the counters can be adjusted accordingly depending on the measurement scale (Ts: the time unit reported by the sensor) and the total measurement time (Ttotal). For example, if Ts is 1 h and Ttotal is one year based on the specification of an IC, a 38-bit counter will meet the requirement to count the usage time from 20 ns (assume system clock = 50 MHz) to 1 h and a 14-bit counter2 will count the usage from 1 h to 8760 h.

![Antifuse Sensor](image)

**Figure 2: Antifuse Sensor**

![Overall Block of Antifuse(AF) Sensor](image)

**Figure 3: Overall Block of Antifuse(AF) Sensor**

As the data stored in registers (counters) could be lost or reset when power supply is off, non erasable memory is required in this sensor. An embedded AF OTP block is used instead of a field-programmable read-only memory (FEPROM) to store the usage time information because FEPROM could be tampered or altered by attackers. In the AF block, prog is assigned to be 1_b1 if the value in counter increases by 1. Through connecting the output of counter2 to address in the AF block directly, the related AF cell will be programmed as 1. Therefore, the largest address of the cell whose content is 1 will be the usage time of CUT based on the measurement scale setup by counter. From the above description, the size of the AF block will be reduced using two counters. Program and read operations, however, share the same address signals in AF block. Therefore, a MUX (MUX1), controlled by data read module, is used to select the address (AF cell) to be read or programmed. Every time power supply is on, the AF block will work in read mode for a short period. During this time, the read address generated by data read module will go through MUX1 and all the AF cells will be traversed based on the traversing binary tree principle.

Once we get the previous usage time, it will be stored in register Reg3 and sent to the adder. The reason for using an adder here is that counters start from 0 every time the power is turned on and the previous usage time must be considered when we calculate the total usage time. In addition, Reg1 is used to sample the data in adder, Reg2 delays the data in Reg1 with one system clock, and XOR gates are used to compare the data in Reg1 and Reg2. If they are different (denoting the
usage time increased), the AF OTP block will work in program mode and the data in Reg1 will go through MUX1 to the address in the AF block. Therefore, combined with the value in counter (the usage time after power-on), the new total usage time will be stored in the AF OTP block by programming a new AF cell with a larger address. From this discussion, the AF OPT block is programmed internally. Through designing our sensor in this way, we can reduce the probability of altering or tampering attacks on the AF-based sensor.

To eliminate the need for additional pins for authentication purposes on the chip, our CAF-based sensor uses a MUX (MUX2) and an authentication (Aut.) pin to send the usage time to the output pins of ICs. Thus, no extra output pins will be added to the original design. When the IC works in normal functional mode, original primary outputs will go through MUX2. If the IC is in authentication mode by enabling the authentication signal, the data read module will set the AF IP in read mode and the usage time will go through MUX2. In addition, when the IC works in manufacturing test mode, the functionality of our CAF-based sensor will be disabled and structural fault test patterns will be applied to the sensor.

B. DATA READ ALGORITHM

```c
initial address = (N/2);
for (I = log (N/2), I > 0, I--)
{
    if ([address] == 1)
    {
        address = address+1;
        if ([address] == 0)
        {
            address = address-1, $stop;
        }
        else
            address = address-2(i-1);
    }
    else
        address = address-2(i-1);
}
```

The speak to is greater than before or decreased by $2i-1 \{i = 0 \ldots \log(N/2)\}$ for the ith loop based on the value in the converse to. If the value stored in the deal with is 1 ([address] == 1) and the value stored in the next lecture to is 0, the take in hand will stand for the usage time previous to power-on based on $T_s$. The read action will last less than log (N/2) + 1 system clock cycle, depending on the value stored in the AF block; this time will be recorded by counter.

C. RO (RING OSCILLATOR SENSOR)

![Figure 4: Ro](image)

The position and worried ROs are the same; both are self-possessed of HVT mechanism. The inverter could be replaced by any other types of gates only if they can make an RO. Sleep transistors are used to fix the ROs to the control supply in the RO-based sensor; PMOS sleep transistors be in incriminate of the bond connecting VDD and the inverters and n-type MOS slumber transistors direct the association flanked by VSS and the inverters. Both the orientation and the harassed ROs work in three modes that are forbidden by the mode sign. Our major objectives of the RO-based sensor areas follow:

- The sensor has to age at a very high rate to help notice ICs used for a small period.
- The sensor must knowledge no aging or insignificant aging during developed test.
- The crash of procedure variations and hotness on RO-based sensor must be negligible.
- The sensor must be elastic to attacks.
- The breadth procedure has to be complete using low-cost gear and be very fast and easy.

![Figure 5: Overall Process of Ring Oscillator](image)

The three modes of operation the occurrence dissimilarity flanked by the compass reading and under duress ROs will be larger over time as the direction RO cannot be gated on by...
you. It is extremely hard for adversaries to strength the RO-based sensor to function in endorsement mode when it is hypothetical to be in its normal functional mode, which would eliminate the aging dissimilarity. The only method to do that would be to modify the original RO-based sensor module, which is impossible during a simple recycling process. A real ring oscillator only requires power to operate; above a certain threshold voltage, oscillations begin on fancy. To augment the timekeeping of undulation, two methods may be used. Firstly, the practical voltage may be increased; this increases both the frequency of the fluctuation and the power inspired, which is dissolute as heat.

III. ADIABATIC SWITCHING

Thermodynamic means no heat transfer. Instead of dissipating power reuse it. By externally controlling the length and shape of signal transitions energy spent to flip a bit can be reduced to very small values

A. RULES TO FOLLOW

✓ Never use diodes since they are fundamentally thermodynamically irreversible
✓ Do not turn on the MOSFET when there is significant potential difference between source and drain
✓ Do not turn off when there is a significant current flowing through the device

Adiabatic design is an energy efficient way of design for low power circuits. Asymptotically zero energy can be obtained by using fully adiabatic circuits at the cost of complexity. Quasi adiabatic logics can be used with minimum energy loss and less complexity.

IV. POWER DISSIPATION

Power reduced by reducing \( V_{dd} \), \( f \), \( C \) and also activity. A signal transition can be classified into two categories
✓ A functional transition and
✓ A glitch

A. GLITCH POWER DISSIPATION

Glitches are temporary changes in the value of the output – unnecessary transitions. They are caused due to the skew in the input signals to a gate. Glitch power dissipation accounts for 15% – 20% of the global power. Basic contributes of hazards to power dissipation are

Hazard generation
Hazard propagation

balancing techniques. Hazard propagation can be reduced by using less number of inverters which tend to amplify and propagate glitches

B. MECHANISM

Mechanisms of power dissipation are usually divided into two classes: dynamic and static power dissipation. Dynamic power dissipation occurs when the circuit is operational, i.e. the circuit is performing some task on some data. Static power dissipation becomes an issue when the circuit is inactive or in a power-down mode. Power dissipation is unavoidable especially as technology scales down. Techniques must be devised to reduce power dissipation. Techniques must be devised to accurately estimate the power dissipation. Estimation and modeling of the sources of power dissipation for simulation purposes. During operation circuits waste energy. There are three major causes of power dissipation in integrated circuits:

C. DYNAMIC

Power consumption which is caused by diabatic charging and discharging of (usually parasitic) capacitances. Dynamic power dissipation can be further subdivided into three mechanisms: switched, short-circuit, and glitch power dissipation. All of them more or less depend on the activity, timing, output capacitance, and supply voltage of the circuit. The repeated charging and discharging of the output capacitance is necessary to transmit information in CMOS circuits. This charging and discharging causes for the switched power dissipation. The power consumption of a CMOS digital circuit can be represented as:

\[ P = fCV_{dd}^2 + fI_{short}V_{dd} + I_{leak}V_{dd} \]

Where \( f \) is the clock frequency, \( C \) is the average switched capacitance per clock cycle, \( V_{dd} \) is the supply voltage, \( I_{short} \) is the short circuit current and \( I_{leak} \) is the leakage current.

D. STATIC

Power consumption which corresponds to the non-zero current of transistors in off state in digital circuits or the biasing current in their analog counterparts. The static power components become important when the circuits are at rest, i.e. when there is no activity in the circuits and they are all biased to a specific state. The static power dissipation includes sub threshold and reversed biased diode leakage currents. Due to the necessary but harmful (in a leakage power sense) down-scaling of threshold voltages, the sub threshold leakage is becoming more and more pronounced. Below the threshold voltage, in weak inversion, the transistors are not correctly off. The sub threshold current has a strong dependence on the threshold voltage.

E. SHORT-CIRCUIT

Power consumption caused by the crow-bar current flowing during the lapse of time when both PMOS and NMOS
transistors are in the on state. In real circuits signals have non-
zero rise and fall times which causes both the P net and the N
net of the CMOS gate to conduct current simultaneously.

This leads to the flow of a short-circuit current for a short
period of time. The input and output slopes of a gate should be
equal to minimize the overall short circuit dissipation in gates.
Also large load capacitance can significantly reduce the short-
circuit dissipation of the driving gates.

V. FLOW CHART

VI. CONCLUSION

The incidence differentiation between the situation and
the strained ROs in the RO-based sensor made the easy
detection of second hand ICs promising. The tradition time
stored in the AF reminiscence using AF based sensors could
show how long an IC had been worn and then recognize a cast-off IC. Investigational results and psychoanalysis
established the efficiency of these sensors. Our prospect work
includes: analyzing the crash of aging revival on the efficiency
of the RO-based sensor; implementing the AF-based sensors
on test chip to additional confirm their usefulness; and
mounting on-chip sensors to notice used analog and digital IC.

REFERENCES


Figure 6: Flow chart of AF Sensor

Figure 7: Overall process of Chart