Active Defense against Counterfeiting Attacks through Robust Antifuse-based On-Chip Locks

Abhishek Basak, Yu Zheng and Swarup Bhunia
Department of EECS, Case Western Reserve University, Cleveland, OH 44106
(axb594, yxz402, skb21)@case.edu

***Abstract*— The rapidly rising incidences of counterfeit Integrated Circuits (ICs) in the semiconductor supply chain pose a significant threat to the electronic industry. These ICs may suffer from functional, performance or reliability issues and can affect design houses, chip manufacturers, system designers as well as end users. The standard chip/package/system level tests are often inadequate in detecting various forms of counterfeit ICs. On the other hand, design approaches that enable IC authentication are often not attractive due to significant design effort, hardware overhead and test cost. In this paper, we propose a novel defense against counterfeiting attacks through a "chip locking approach", where an IC is made non-operational by locking select pins through insertion of Antifuse (AF) devices in input/output circuitry. It can be unlocked through application of a hard-to-clone key. The key is internally stored in a one-time programmable non-volatile memory. The key storage and comparison circuit is protected against reverse engineering and side-channel analysis attacks. Through mathematical analysis and simulation results, we demonstrate that the proposed mechanism provides high level of protection against all major forms of counterfeiting attacks (reselling, remarking and cloning) at ultralow overhead ($< 0.01\%$ area).**

I. Introduction

A counterfeit Integrated Circuit (IC) is an electronic component with discrepancy on the material, performance or characteristics, but sold as a legitimate chip. It can be an unauthorized copy, remarked/recycled die (e.g. used chip sold as new), cloned design at untrusted foundry, or a misrepresented, failed real part. Counterfeit ICs can have altered functionality, poor performance or degraded reliability of operation. The significant rise in counterfeit ICs is a major concern to chip designers, system integrators as well as end users in the semiconductor industry [1], [2]. The cost of counterfeiting and piracy is estimated to rise to 1.2 to 1.7 trillion dollars by 2015 [1].

The increasingly complex global semiconductor supply chain, spanning different countries and their legal systems to meet the ever-rising demand, provides ample opportunities for adversaries to insert counterfeit chips in the market. Prior to actual deployment, an IC is often bought and resold many times. Purchasers rely on brokers, who in turn buy from untrustworthy entities including online forums [2]. The various sneak channels offered by the current semiconductor business model (Fig. 1(a)) that can be exploited by an adversary are shown in Fig. 1(b). The two major categories of counterfeit ICs are *1) remarked/recycled*, 2) *cloned new parts*. The former includes the selling of aged chips as

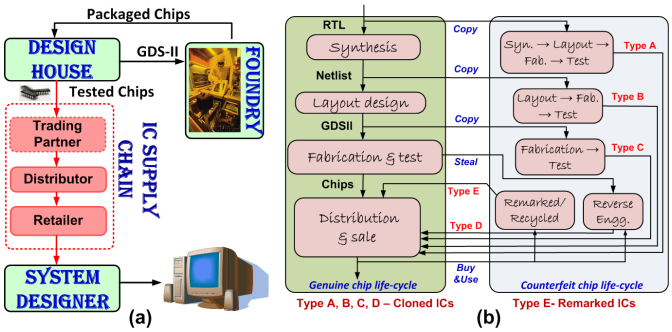

Fig. 1. a) Present semiconductor business model; (b) possible sneak channels utilized by adversaries to insert counterfeit ICs in the supply chain.

new in the open market, after possibly repackaging and relabeling of the die. According to a recent report, over 80% of the counterfeits chips are either recycled or remarked [3]. The latter category includes unauthorized production of an IC without legal rights. It is typically performed through IP piracy at different levels (shown in Fig. 1(b)), over production or reverse engineering of an IC. The standard chip tests are often inadequate in detecting various forms of counterfeit ICs. Besides, the existing design-for-counterfeit prevention approaches are often not attractive due to inadequate coverage of counterfeit chips and/or significant design/test effort as well as hardware overhead. Hence, to address this growing concern, there is a critical need for efficient, low-overhead protection against counterfeit ICs.

In this paper, we propose a novel anti-counterfeiting approach based on die-level locking using antifuse (AF) devices. It provides active defense against various forms of counterfeiting attacks. The key idea is to lock an IC by placing AF devices in input/output port circuitry of select pins on die. An AF behaves as a normally open switch (up to $\sim 1G\Omega$) until programmed [4], thus disabling the pin. A locked IC in the supply chain remains non-operational until unlocked by a proprietary programming device that applies a secret unlocking key to program the AFs. Fig. 2(a) illustrates the implementation of the locking mechanism. As AFs are one-time-programmable (OTP), the approach automatically protects against reselling of aged/scavenged chips. By using a hard-to-clone, IC family specific key to program the on-chip AF devices, the approach also achieves robust protection against cloning attacks. Unlike the existing approaches, the proposed solution provides the following key advantages:

978-1-4799-2611-4/14/$31.00 ©2014 IEEE
IEEE computer society

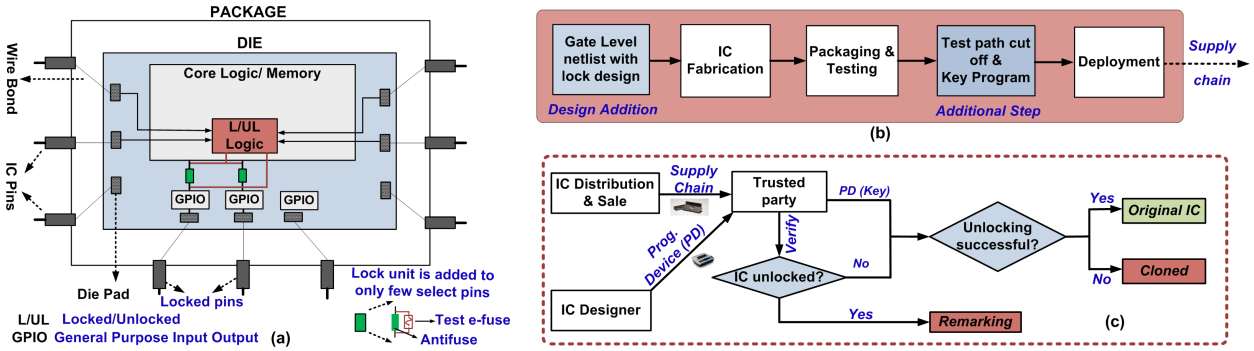

Fig. 2. a) Implementation of the proposed on-die locking mechanism in an IC; b) incorporation of the security mechanism in the current IC design cycle and c) the semiconductor business model to protect against diverse counterfeiting attacks.

(1) it provides an active defense against counterfeiting attacks; (2) it protects against both reselling/remarking as well as cloning attacks - two major forms of counterfeit chips in a supply chain; and (3) it incurs significantly less design/hardware overhead. The modifications required in a IC design cycle for addition of the locking mechanism are shown in Fig. 2(b). Besides the insertion of the locking scheme in the design before manufacturing, the extra step includes test path cut off in AF pins and key programming prior to deployment. This step is performed under the control of the IC designer and hence secure. Post-fabrication programming of the key prevents cloning by soft or hard intellectual property (IP) piracy (Types A, B, C in Fig. 1(b)).

Like other anti-counterfeiting schemes, our proposed locking mechanism seamlessly fits in the current semiconductor business model. The proprietary programming device would reside only in the hands of the trusted parties e.g. a system designer (e.g. computer manufacturer) or a last level retailer (e.g. Digikey). They would unlock the chips and utilize them in their systems or supply to the end customer respectively. The detection of counterfeit ICs using this scheme, in the present business model is summarized in Fig. 2(c). In particular, the paper makes the following major contributions.

- It proposes an active antifuse-based chip locking scheme that can effectively protect against counterfeit chips, specifically reselling/remarking as well as design piracy and reverse-engineering based cloning attacks.
- It provides detailed implementation of the approach including choice of antifuse and select pins, design of the programming circuit, locking/unlocking mechanism and protocols. It considers protecting the unlocking signature against invasive as well as side-channel attacks. The design modifications include a OTP non-volatile memory (NVM) to store a $64/128$ bit key and the electronic circuitry to compare a supplied input sequence (by system designer or last level retailer), to proceed to the AF program phase, in case of a match with the key.
- It presents comprehensive security and overhead analysis to demonstrate the robustness of the approach against various forms of counterfeiting attacks. It compares the hardware overhead of the proposed approach with major alternative approaches. It shows that it provides high level of unified protection at a very small overhead.

II. Related Work

Existing countermeasures against counterfeiting attacks are mostly passive i.e. approaches aiming at detection of counterfeit chips through test/validation steps. In case of remarked ICs, the detection approaches mainly involve physical tests such as external package inspection, decapsulation verification and material analysis. However, most IC packages are carefully modified such that they can easily evade these tests [1]. Cloned chips are tested for design specifications by functional tests, DC/AC parametric tests and burn-in tests for reliability verification. These are expensive and difficult to perform exhaustively for all ICs. There are attempts to tag each chip with a unique ID e.g. an encrypted number for each IC with a RFID tag. However, present reverse-engineering tools have become very advanced, allowing an attacker to read these IDs [2].

Hence, active approaches based on appropriate design modifications to prevent counterfeiting attacks have emerged more attractive. They include on-chip aging sensors [5] and physical unclonable functions (PUF) [6]. Aging sensors can however work only for isolating recycled/used chips. Moreover, they typically incur significant design and test efforts as well as area/power overhead [2]. PUFs, on the other hand, exploit intrinsic, unclonable random variations in the manufacturing process to generate unique identifier for each chip. However, they cannot protect against used chips. Moreover, PUF signatures are often not robust in the presence of temperature and voltage fluctuations as well as aging-induced device degradation. Most PUFs also incur considerable design effort, hardware overhead, and test workload for the manufacturer. Hardware metering solutions [7] can provide active defense against cloning attacks. However, effectiveness of metering in case of scavenged, remarked chips are not well studied. Furthermore, active metering approaches rely on presence of a robust random generator circuit, which considerably adds to the hardware overhead. The proposed solution presents a novel unified active defense against both reselling and cloning attacks at much lower hardware overhead compared to alternative approaches.

TABLE I

MAJOR ELECTRICAL PROPERTIES OF THE ANTIFUSE BASED LOCK [4]

Parameters	Value
Programming voltage	4-6 V
Programming current	5-15 mA
Programming duration	0.1-5 ms
OFF state resistance	$50M\Omega - 1G\Omega$
ON state resistance	$20\Omega - 80\Omega$

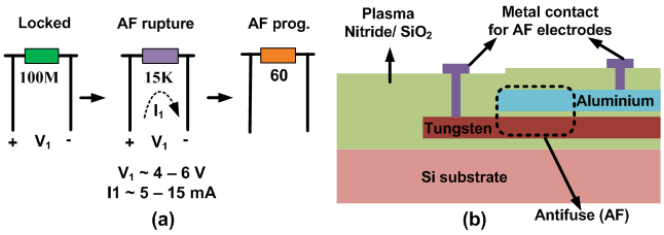

Fig. 3. a) Steps in programming an antifuse [8]; b) Implementation of MIM antifuse in 2 metal process.

III. DIE LEVEL CHIP LOCKING MECHANISM

A. Pin Lock Structure

The lock component, which renders the pin/s non-operational is the antifuse (AF). AFs are one time programmable elements (OTP), behaving as a normally open switch (resistance $> 100M\Omega$) [4] in the un-programmed state. Once the programming voltage is applied across the terminals, irreversible changes occur in the structure of the AF, leading to the formation of a conductive filament, hence behaving as a closed switch (resistance $\sim 50 - 1K\Omega$) [8]. AFs have been in use in secure, reliable programmable read-only memory (PROM) and military grade field programmable gate arrays (FPGA) [8]. Among possible AF structures, we choose Metal-Insulator-Metal (MIM) ones due to their low on-state resistance and capacitance, and lower breakdown voltages [4]. The electrical properties of the chosen MIM AF structure, are presented in Table I. The steps in the AF programming, with the corresponding electrical parameters are shown in Fig. 3(a). The cross-sectional area of AFs are below $0.1\mu m^2$ (determined mainly by contact sizes) at advanced process nodes, and hence minimal area overhead. In a fabrication process as shown in Fig. 3(b), MIM AFs incorporating tungsten, aluminum electrodes and plasma nitride/silicon dioxide [8] insulator are deposited over the silicon substrate. Consequently plasma and DRIE etching are performed for the metal electrode contacts.

B. Lock Insertion in I/O Circuitry

To render a desired pin non-operational by the proposed locking scheme, an AF device would be inserted in the input/output (I/O) circuitry between the pad and the corresponding port data line. Among IC pins, those that may be selected for locking include general purpose input/output (GPIO) as well as input or output only pins. Power supply pins would be required for key programming and chip unlocking and hence not locked. Besides, clock pins are not considered to avoid any possibility of frequency degradation, jitter etc. The placement of an AF in the input path of a GPIO pin of a state of the art micro-controller is shown in Fig. 4. The possible locations for lock insertion in the output path of the port are shown as well. The illustrated GPIO structure is a good representation of the I/O circuitry commonly found in processors, FPGAs and micro-controllers. When the port acts as an input, the output driver is in the high impedance state and the data bit is read through the input latch and buffer. In the output mode, the data in the latch is transferred to the pad. The extra locking signals to the port circuit are the program high (PH) and low (PL) voltages to the AF and the program enable (PE) to the buffers. For all locked pins, a test path comprising of an OTP e-fuse [9] is placed in parallel to the AF (as shown in Fig. 4) for use during chip testing. After post-package validation, the test path is disabled by blowing the e-fuse in a secure, trusted process. Hence, an adversary cannot utilize test paths for causing malfunction or functional reverse-engineering. When the chip is functional, the AF program buffers are always in the high impedance state, and hence no interference occurs in the normal input-output operations. The AF is placed after the buffer and not directly near the pad to avoid any remote possibility of alterations of AF state due to environmental interference (voltage, EMI, stray signals etc.) through the pads.

C. Programming the Key

Post fabrication, the authentication key is programmed into each IC. One Time Programmable (OTP) Read Only Memories (ROM), based on Metal Oxide Semiconductor (MOS) gate capacitor Antifuses (AF) [10], [12] are chosen due to no extra process steps and higher reliability at advanced process nodes, compared to flash and PROM structures. The structure of such an AF based NVM array with minor design additions for our application is shown in Fig. 5(a). Here, we select only one key bit operation per cycle for programming and

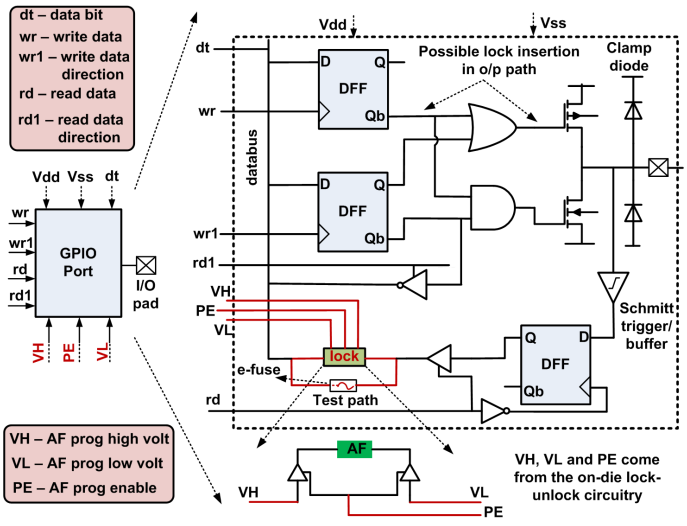

Fig. 4. Insertion of the lock unit in a general purpose input-output (GPIO) port of a state of the art microcontroller [11].

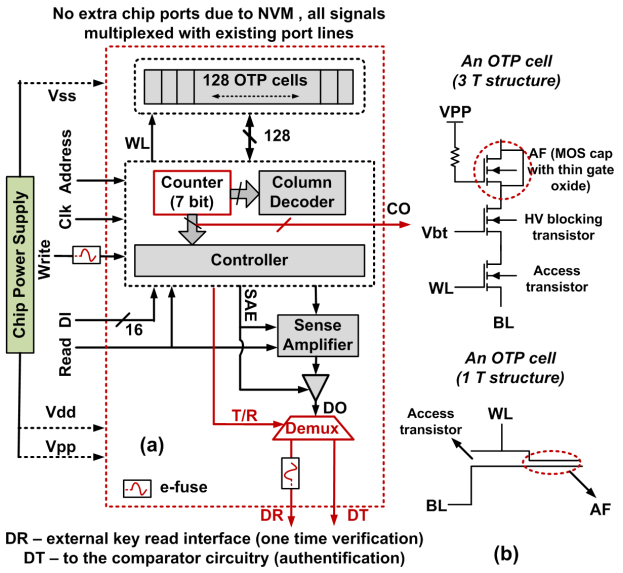

Fig. 5. a) Modified OTP antifuse 128-bit ROM for storing authentication key [12]; b) 2 possible OTP ROM bit structures [12], [13].

comparison, to minimize hardware overhead. The internal controller logic maintains the transitions between different states. For key programming, the write signal is enabled. The address bits of the column decoder are controlled by a counter. Successful implementation of the locking method requires the prevention of external key read out in field by an adversary. After programming, based on an enabled test signal (T/R) to a de-multiplexer by the controller, the key bits are read out once through the external read line (DR) for validation. Consequently, DR is disabled by programming the OTP e-fuse. During IC authentication, T/R signal is disabled by the controller, passing the individual key bit values through DT to the lock/unlock circuitry for comparison. DT does not have any external access. To prohibit any possibility of field programming of the unprogrammed AFs (cells storing 0), the write signal is disabled by a similar protection scheme. When the legitimate IC reaches a system designer, he/she uses the proprietary device (obtained from manufacturer either directly or a trusted supply chain) to input the key and unlock the AFs in pin. All NVM signal lines are derived from multiplexed original ports to avoid addition of chip ports. Two OTP AF based cells, one a 3T structure and the other a 1T structure, are illustrated in Fig. 5(b) [12], [13]. Due to significant area advantages, we use the latter AF structure, for storage of the key.

D. Design Circuitry for Chip Unlocking

The input sequence for chip unlocking is stored in the proprietary programming device, for each IC family. It is uploaded into the chip via one or few select multiplexed input pins, depending on the design implementation. The comparison circuitry consists of one or many XOR gates and a central controller, transitioning between different lock-unlock states. The key is stored in the OTP NVM with disabled external access paths and the internal read connected to the lock-unlock circuitry. An illustration of the simplest single bit design implementation (ultra-low area overhead) is in Fig. 6. Apart from the OTP AF programming, all circuit components work at normal logic operational voltages, derived from the on-die voltage regulators. The AF cell programming voltages ($Vpp \sim 5V$) in the NVM and lock units [4], [12] are derived directly from the primary supply input. The clock inputs, would be derived from the on-chip PLL/s.

1) Controller State Transitions: The default controller state during field operations is ***Idle***. On the first sequence bit/s input, the start conversion (SC) signal is enabled by the programming device. This also enables the key bit read from the NVM (for multi-bit comparison per cycle, parallel sense amplifiers, buffers, column decoders are necessary). With this, the state machine transitions to the ***Comp*** state for bitwise key match, using the XOR gate/s. Depending on the output/s and the number of bits compared (by the NVM counter), the controller decides the next states i.e. if the bits match, the next higher order bits are compared in the Comp state, where as the comparison operation is halted in case of a unequal bit value case (Idle state restored). In the scenario of equality of all the bits, the Program Enable (PE) signal is made high (***Prog*** state), which enables the antifuse (AF) electrode voltage lines and the program buffers for unlocking of the pins. After a time count, determined by the AF programming duration, the PE signal is made low, and the controller returns back to the default Idle state. This duration would be counted by the same NVM counter (previous count finished), by the PE signal feedback to the NVM. The controller state transition diagram, for 128 bit key is shown in Fig. 7(a), for a simple single bit comparison per cycle. Apart from SC, the state input signals are the XOR gate output CE, the count of number of bits compared CO and the count of programming duration PT (assumed 5 bit).

IV. Security and Overhead Analysis

A. Security Analysis

Aged, recycled chips in the supply chain can easily be identified from the broken locks. In such scenarios, the chip gives functional outputs corresponding to input sequences, signifying already programmed locks and hence an used IC. Besides, pin level parametric failure tests such as input high

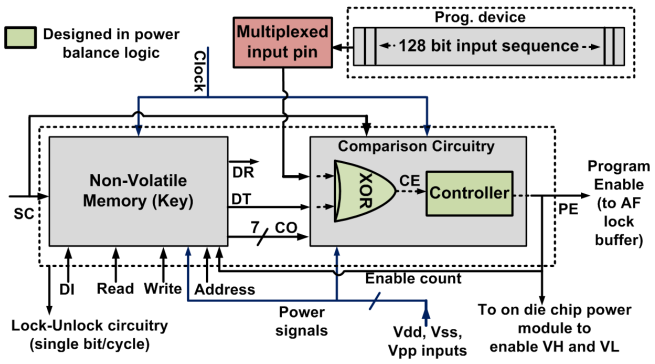

Fig. 6. Additional design circuitry for storage and comparison of key for counterfeit chip detection.

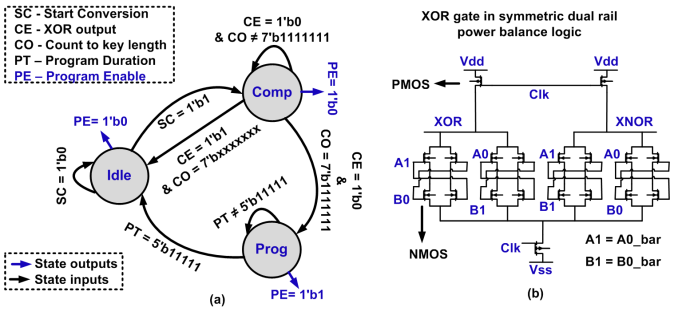

Fig. 7. (a) State transition diagram of the controller in the comparator circuitry; (b) A XOR gate in Power Balanced Precharge logic [17].

and low (IIH and IIL) leakage, continuity tests can be utilized to distinguish between broken, absence, incorrectly copied or legitimate locking scheme. For cloning ICs, an adversary may steal the modified IP with lock design, at the RTL, gate or foundry level as well. Hardware obfuscation based approaches have played a role in preventing the first two with a varying degree of success [14]. In our proposed scheme, the post manufacturing programming of the key in the AF based non-volatile memory (NVM), with disabled external read and program paths, prevents cloning of the IC with only the stolen IPs at different design levels. To successfully clone a design, an attacker has to exactly decipher the key to enable programming of the copied IC with the proprietary device, and hence evade detection. Assuming an attacker supplies completely random binary patterns, the probability of each bit in the input sequence to be 0 or 1 is $1/2$. Hence for a N bit key, the probability of a match, for a particular independent input trial is $1/2^N$ [15]. Hence deciphering a 64 or 128-bit key would require 2^{64} or 2^{128} functional trials in the worst-case, and hence practically infeasible. Side channel based attacks can also be resisted successfully, as discussed in the next section. So die level destructive reverse-engineering, which is extremely complex and expensive [16], would be the only way for an adversary, to decipher the design.

1) Resistance against Side Channel Attacks: As in encryption algorithms, although the proposed methodology is extremely resistant to mathematical reverse-engineering, side channel attacks (SCA) can in some scenarios reveal the secret stored key by utilizing the actual implementation of the lock-unlock logic circuitry. SCA techniques like differential power analysis (DPA) can utilize the input data dependent logic transitions and hence power consumption, to decipher part or whole length of key [17]. To protect against such attacks, we propose to employ the following steps.

- *Full Key Comparison:* To prevent any input sequence dependent timing, current and hence power signatures, in all input scenarios, the controller would compare the entire length of the key and sequence, to transition to either the Program or Idle state. A separate signal *Mismatch* would be enabled on the first bit inequality. On comparison of all bits, if Mismatch is low, pin unlocking is enabled. Otherwise, the Idle state is restored.
- *Power-balanced Logic:* To prevent input data dependent power consumption patterns, the XOR gate for key bit comparison and the controller circuitry are implemented in a *Power Balanced* logic style. An implementation of a XOR gate in power balanced, pre-charged logic style is shown in Fig. 7(b). Like dynamic differential logic, they lead to equivalent switching capacitance every cycle irrespective of input transitions [17].

2) FSM based Unlocking: Instead of a stored-key, a finite state machine (FSM) based approach can also achieve equivalent security against functional reverse-engineering. Here, the programming is enabled on application of a pre-defined sequence of inputs. If the program state is reached on N transitions for a M bit input stream, the required number of trials is $2^{(M*N)}$ [15]. For a 8-bit input and 16 states, the complexity is 2^{128}. However, the drawback of using FSM is that an adversary in the foundry may clone the design with the FSM. The proposed post-fabrication programming of the key makes the scheme resistant to such foundry level attacks.

3) Security against Overproduction: Another form of counterfeiting attack is overproduction of ICs by an untrusted fabrication house without the knowledge of the designer. In our proposed scheme, the key programming is done at the end of the IC design cycle after testing and test path cut off in a secure fashion. Post manufacturing, overproduced ICs follow a different path into the supply chain. When such an IC reaches the hands of a system designer/retailer, the inability to unlock it with the proprietary key (if chip is non-operational) categorizes it as a cloned chip. If the test fuses are left unprogrammed, the ICs would function, thereby being classified as a recycled chip. Hence the proposed scheme also offers protection against overproduced chips.

B. Overhead Analysis

The key is stored on-die in the OTP AF based NVM, the unlocking sequence from the programming device is input through multiplexed input/s, and finally a XOR gate and controller are used for comparison. This design has been functionally simulated using Model Sim, for a 16 bit key for 2 input sequences, one equal and one unequal to the key. The controller transitions through 3 states as described, with a 5 bit program duration variable. The same design has been scaled up to a realistic scenario of a 128 bit key and synthesized at 45 nm with the low power NCSU PDK45nm technology library to obtain an estimate of the area overhead of the lock mechanism. The overhead values for three key lengths, in three ICs are tabulated in Table II. The 3 ICs

TABLE II
SECURITY & AREA OVERHEAD OF PROPOSED LOCKING AT 45 NM

	32-bit key	***64-bit key***	***128-bit key***
No of trials	2^{32}	2^{64}	2^{128}
Lock Area (μm^2)	215	245	295
Core-i7 (%)	$8.1 * 10^{-5}$	$9.4 * 10^{-5}$	$1.09 * 10^{-4}$
OMAP3630 (%)	$1.20 * 10^{-4}$	$1.38 * 10^{-4}$	$1.59 * 10^{-4}$
Spartan 6-LX (%)	$2.17 * 10^{-4}$	$2.47 * 10^{-4}$	$2.88 * 10^{-4}$

TABLE III
QUALITATIVE COMPARISON WITH ALTERNATIVE APPROACHES

Property	PUF [6]	Aging Sensor [18]	**Proposed Method**
Implementation level	On-Die	On-Die	On-Die
Signature specificity	Per IC	N/A	Per IC family
Used/Remarked IC det.	No	Yes	Yes
Cloned IC det.	Yes	No	Yes
Die area overhead	High	High	Low
Test workload (designer)	High	Medium	Low
Difficulty of cloning sig.	Very High	N/A	High
Robustness	Medium	Medium	Very High

considered are the Intel Core-i7 general purpose processor, TI OMAP3630 embedded processor and Xilinx Spartan 6-LX FPGA, all fabricated at 45 nm process technology. The overhead due to a $32/64/128$ bit AF based OTP ROM with peripherals, for key storage,is incorporated into the calculations [12]. Besides, the area in the I/O circuitry due to AF and program buffers in 30% of the total pins is added as well. The cross sectional areas of MIM AFs are dominated by the contact sizes ($2\lambda X2\lambda$) and hence minimal.

From Table II, it is observed that the locking mechanism incurs negligible area overhead ($\ll 0.001\%$ in state of art chip designs). On doubling the signature length, the reverse-engineering complexity increases exponentially, whereas the area overhead increases linearly up to a maximum value of 0.0003% for a 128-bit key. For fast unlocking, we can easily utilize parallelism (sense amplifier, decoder, XOR) with insignificant overhead. Besides, the programmed AF resistances in MIM structures are small (20-80Ω) [4] to cause any loading effects in the chip pins. Hence the proposed mechanism provides extremely high protection against various forms of counterfeiting attacks, at negligible overhead.

C. Comparison with PUF and Aging Sensors

Two other well-known design techniques for protecting against counterfeit chips are PUF (e.g. RO-PUF [1] or MECCA PUF [6]) and the aging sensor, typically realized with differential oscillator [18]. Although theoretically the PUF signature is extremely difficult to reverse engineer, it has certain disadvantages with respect to protection against counterfeiting attacks. Aging sensors, on the other hand, incur significant design overhead. Table III provides a qualitative comparison between our proposed locking mechanism, PUF and aging sensors. Estimated area overhead values of RO-PUF [6] and an aging sensor [18] are compared with the 128-bit key based locking method. As seen from Table IV, our proposed method incurs much lower ($< 10\%$ of the other two) area overhead. Besides, although the BFSM of the active hardware metering approach incurs comparable low overhead [7], a PUF structure is needed for random ID generation, and hence overhead would be significant.

TABLE IV
AREA OVERHEAD COMPARISON AT 45 NM. PROCESS

	Proposed (128-bit key)	***RO-PUF*** [6]	***Aging Sensor*** [18]
Area Overhead	$295\mu m^2$	$3122\mu m^2$	$4190\mu m^2$

V. CONCLUSION

We have presented a design approach for active protection against counterfeiting attacks through locking select pins of an IC by antifuse devices (AFs). A system designer can unlock a chip before using it in a system by a key-based programming of the AFs with a proprietary programming device. Unlike existing approaches based on aging sensors and PUFs, it simultaneously protects against two major forms of counterfeiting attacks, namely reselling and cloning. Use of AF as locking mechanism ensures one-time unlocking - i.e. once unlocked, an IC remains unlocked through its life cycle. Hence, the proposed approach can readily prevent reselling of aged/scavenged chips. We have shown that the unlocking signature with a $64/128$ bit key is practically infeasible to functionally reverse engineer. Hence, it also protects against different forms of cloning attacks. We have presented detailed analysis on the on-die implementation of this locking methodology. The key matching circuit is designed to be robust against both invasive and side-channel attacks. The effectiveness and overhead of the approach is compared with alternative anti-counterfeiting approaches. Future work would include integration of the locking approach with other design-for-security approaches and hardware prototyping of the locking methodology in a realistic IC.

REFERENCES

[1] M. Tehranipoor et. al, "Counterfeit IC Detection and Challenges Ahead", *ACM SIGDA*, Mar 2013.
[2] Y. Makris et. al, "Counterfeit Electronics: A Rising Threat in the Semiconductor Manufacturing Industry", *ITC*, 2013.
[3] "Chip counterfeiting case exposes defense supply chain flaw", *http://www.eetimes.com/*.
[4] W. T. Li et. al, "A Comparative Study of the OnOff Switching Behavior of Metal-Insulator-Metal Antifuses", *IEEE EDL*, Vol. 21(6), 2000.
[5] X. Zhang et. al, "Identification of Recovered ICs using Fingerprints from a Light-Weight On-Chip Sensor", *DAC*, 2012.
[6] A. Krishna et. al, "MECCA: A Robust Low-Overhead PUF using Embedded Memory Array", *CHES*, 2011.
[7] F. Koushanfar et. al, "Active Hardware Metering for Intellectual Property Protection and Security", *USENIX Security*, 2007.
[8] C. Hu et. al, "Antifuse structure comparison for field programmable gate arrays", *IEDM*, 1992.
[9] N. Robson et. al, "Electrically Programmable Fuse (eFUSE): From Memory Redundancy to Autonomic Chips", *CICC*, 2007.
[10] H. Ito et. al, "Pure CMOS One-time Programmable Memory using Gate-Ox Anti-fuse", *CICC*, 2004.
[11] "PIC16F84A - Datasheet", *http://www.microchip.com/*.
[12] K. Lee et. al, "A 32-KB Standard CMOS Antifuse One-Time Programmable ROM Embedded in a 16-bit Microcontroller", *JSSC*, 2006.
[13] C. Downing, "1T-OTP - The Ideal NVM Solution for the Growing Mobile Device Market", *http://www.chipestimate.com*.
[14] R. Chakraborty et. al, "Hardware protection and authentication through netlist level obfuscation", *ICCAD*, 2008.
[15] S. Paul et. al, "VIm-Scan: A Low Overhead Scan Design Approach for Protection of Secret Key in Scan-Based Secure Chips", *VTS*, 2007.
[16] "Security Analysis - Analytical Solutions", *http://www.asinm.com/*.
[17] P. Schaumont et. al, "Using Virtual Secure Circuit to Protect Embedded Software from Side-Channel Attacks", *IEEE TComp*, 2013.
[18] C. Kim et. al, "Silicon Odometer: An On-Chip Reliability Monitor for Measuring Frequency Degradation of Digital Circuits", *JSSC*, 2008.