This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

P-Val: Antifuse-based Package-level Defense against Counterfeit ICs

Abhishek Basak and Swarup Bhunia
Department of EECS, Case Western Reserve University
Cleveland, OH 44106, USA
{axb594, skb21}@case.edu

***Abstract*—The rapidly growing incidences of counterfeit integrated circuits (ICs) pose a significant threat to the semiconductor industry. These ICs may suffer from functional, performance or reliability issues and can affect chip manufacturers, system designers as well as end users. The standard chip/package level structural and functional tests are often inadequate in detecting various forms of counterfeit ICs. Moreover, existing design for security approaches are usually not attractive due to additional design modifications, hardware overhead, test cost and inadequate robustness. In this paper, we propose a novel, low-overhead package-level IC integrity validation approach, referred to as *P-Val*, for unified protection against two primary forms of counterfeiting attacks: recycling and cloning. Protection against recycled/remarked chips is achieved through a unique active defense that inserts antifuses (one-time programmable) to few select pins inside the package. It effectively disables the functionality or "locks" these pins, which need to programmed before first-time use to make a chip functional in a system. To protect against cloned ICs, intrinsic random variations in programmed resistances of antifuses connected to some of the remaining IC pins are exploited to create unique chip-specific signatures for authentication. *P-Val* requires no die-level design modifications and remains effective for legacy designs. Moreover, we show that it is effective for small chips with just few pins including analog ICs, where common authentication approaches fail to work. We discuss optimal choice of antifuse structure and program parameters; their integration in IC packages; and the signature generation/verification process. Through mathematical analysis and simulation results, we demonstrate that the proposed mechanism provides high level of protection against counterfeiting attacks at ultra-low overhead ($< 0.05\%$ package area).**

***Index Terms*—Counterfeit ICs, Recycling, Cloning, Antifuse, Package-level, Integrity, Validation, Authentication**

I. Introduction

A counterfeit chip can be an unauthorized copy, remarked/recycled die (e.g. used chip sold as new), cloned design obtained through reverse engineering or piracy, overproduced chip or failed real part. The rising incidences of counterfeit integrated circuits (ICs) in the semiconductor supply chain has emerged as a great concern to the electronic industry [1]. Counterfeit ICs can have altered functionality, poor performance or degraded reliability of operation. They pose a significant threat to chip manufacturers, system integrators as well as end-users in diverse industrial sectors like consumer electronics, automobile, health-care, and networking. Most frequent incidences of IC counterfeiting are not restricted to any particular type, as shown in Fig. 1(a) [2]. It includes processors, FPGAs and analog/mixed-signal ICs. Fig. 1(b) illustrates the number of cloned ICs used in different mission critical systems, sold by a company VisionTech under the name of different vendors [3]. The cost of counterfeiting and

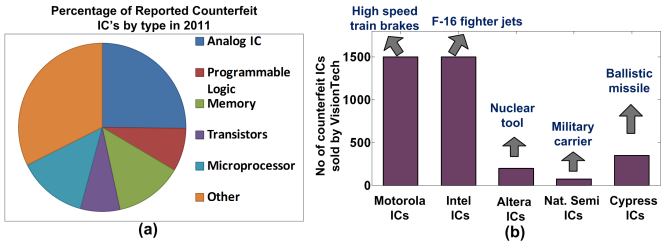

Fig. 1. a) Percentage of reported counterfeit incidences by type in 2011; (b) Counterfeit ICs sold by VisionTech under name of semiconductor vendors.

piracy is estimated to rise to a staggering 1.2 to 1.7 trillion dollars by 2015 [1].

The increasingly complex global semiconductor supply chain, spanning different countries and their legal systems, provides ample opportunities to adversaries to insert counterfeit chips in a supply chain. Prior to actual deployment, an IC is often bought and resold many times, involving untrustworthy entities [2], [4]. The current semiconductor business model (shown in Fig. 2(a)) offers various sneak channels that can be exploited by an adversary, as illustrated in Fig. 2(b). The two major categories of counterfeit ICs are *1) remarked/recycled*, 2) *cloned new parts*. The former includes the selling of aged, used chips as new in the open market, possibly after remarking or some repackaging of the die. Over 80% of the counterfeits chips are reported to be either recycled or remarked [3]. Cloned ICs include unauthorized production of an IC without legal rights, which is usually performed through IP piracy at different levels (Fig. 2(b)), over-production or IC reverse engineering. The standard chip, package and system level tests are mostly inadequate in detecting counterfeit ICs. Furthermore, the existing design-for-security (DfS) approaches are often not attractive due to inadequate coverage of counterfeit chips, or

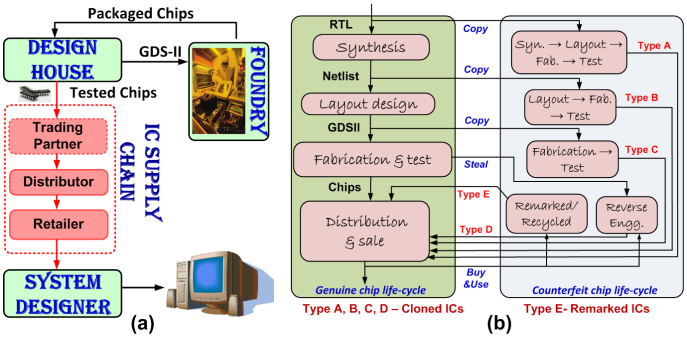

Fig. 2. a) Present semiconductor business model; (b) possible sneak paths for adversaries to insert counterfeit ICs in the supply chain.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

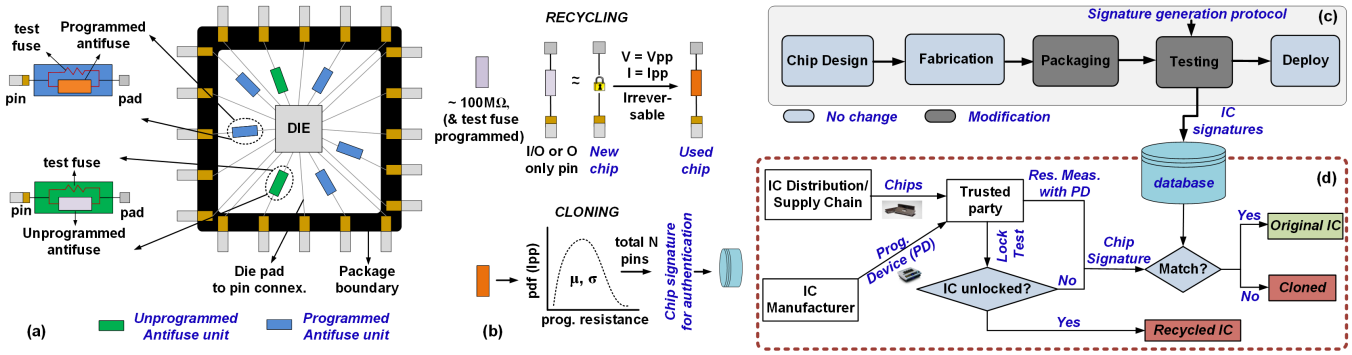

Fig. 3. a) Overview of the proposed security mechanism in an IC; b) unified protection against recycling and cloning; c) modifications required in the IC design cycle to incorporate P-Val; d) the seamless integration of P-Val with the current semiconductor business model for enhanced security.

significant design/test workload, and/or hardware overhead. Moreover, a majority of them are not applicable to legacy designs (finalized designs for production) and analog chips, which comprise a significant portion of the semiconductor market. As a result, many actual counterfeit incidences have not even been reported in recent times. To address this growing concern, there is a critical need for robust and low-overhead protection against counterfeit ICs.

In this paper, we propose a novel, unified, package-level IC integrity validation approach, referred to as *P-Val*, to protect against recycling and cloning of ICs. Protection against used, aged chips is achieved through a unique active defense approach, which involves locking of an IC by insertion of antifuse (AF) devices to one or few select pins of the IC at the package level, as illustrated in Fig. 3(a). AF devices are one-time-programmable (OTP) and commonly used in antifuse based secure Field Programmable Gate Arrays (FPGAs) and non-volatile memories [5]. They behave as normally open switches (up to $\sim 1G\Omega$) until programmed [6]. Hence, an AF device series connected with a pin, can disable IC function (Fig. 3(b), upper), effectively "locking" the IC. Even if one or few pins of a chip are disabled, the IC could lose a significant part of its functionality. A partially functional chip is of no value to a customer (e.g. system integrator/end retailer/user). Parallel test fuses (TF), also integrated at the package level to these locked pins, are used for final chip testing and blown before deployment. The pins selected for locking are usually from the general purpose input/output (GPIO) or output only pin set of the chip as programming them only requires setting a fixed output voltage (e.g. 0 V) at the die pad end and externally applying a program voltage at the pin with consequent passing of program current. Insertion of AFs to one or few select pins during packaging incurs minimal area overhead [5]. A locked IC in the supply chain remains non-operational until unlocked by application of required programming parameters by a trusted party e.g. system integrator. As AFs are OTP, the chip is functional for its entire life cycle once unlocked. Hence, a programmed AF serves proof of past usage/handling and automatically protects against reselling of aged chips of all types, including legacy designs and analog ICs.

For security against cloning, we exploit intrinsic variations in programmed resistance of AF devices connected to IC pins that enable us to create unique chip-specific signatures for authentication (Fig. 3(b), lower). These AFs are integrated into few/all of the GPIO or output pins from the set of pins not used for chip locking, as illustrated in Fig. 3(a). They are programmed after package testing. The chip signature is evaluated and stored in the designer's database just before being deployed in the supply chain. It is well-known that inherent randomness in AF fabrication and programming process leads to variations in the insulator thickness, electrode and insulator composition, heat distribution during program, as well as the stoichiometric composition of the final filament [7]. As a result, the programmed resistance of AFs exhibit intrinsic random variations around nominal values for manufacturing and program parameters [8], [9], which are utilized to create the chip-specific signatures. As lower program currents (I_{pp}) of the chosen AF structure leads to higher variations (better uniqueness of signatures) and currents greater than I_{pp} leads to irreversible programmed resistance variations, test fuses (TFs) are also implemented in parallel to the authentication pin AFs for final chip test (full test coverage) before they are blown. Consequently the authentication AFs are programmed.

Unlike most existing DfS solutions, P-Val does not incur any die-level overhead and can be applied to legacy designs, which is a major portion of the market. It only requires commensurate modifications at the package and testing phases as illustrated in Fig. 3(c). To clarify, for ICs based on these legacy designs, already employed in systems in the market, P-Val based protection does not apply due to requirement of minimal, yet some package modifications and generation of signature before deployment. The AF-TF pairs can be integrated into various types of chip packages through low-overhead steps as discussed in Section III. The package area overhead (due to AF-TF) is negligible ($< 0.05\%$) even for protection schemes involving all of the IC candidate pins. P-Val is flexible for application to chips of various types including analog and mixed-signal ICs, for which integration of conventional security primitives, e.g. physical unclonable functions (PUFs) can be prohibitively expensive. The proposed security approach seamlessly integrates with the current semiconductor business cycle as illustrated in Fig. 3(d). An optional programming and verification device (PD) may be securely exchanged between the chip designer and a trusted party like system integrator to facilitate AF programming and signature verification. Finally, P-Val is transparent to the end-user i.e. it

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

comes at no constraints with regards to usage and performance. The candidate pins, AF, TF properties are chosen such that any loading effects at the corresponding pins are minimal during normal chip operations. As almost all counterfeiting attacks arise in the supply chain, IC authentication is considered only till the system designer level i.e. the threat model for P-Val covers the entire untrustworthy supply chain, but in-field authentication is not considered in the current work. In particular, the paper makes the following key contributions:

- It proposes a novel package-level design approach using AF devices that can simultaneously protect against two major categories of counterfeiting, namely recycling and cloning. To the best of our knowledge, this is the first package-level anti-counterfeit solution.
- It provides detailed implementation of the approach including integration with semiconductor business cycle, choice of AF, TF structure, program properties and fabrication in different IC package types.
- Through mathematical analysis and simulation results, it shows that the proposed approach provides high level of security at zero design modifications, while incurring minimal package area overhead. P-Val can be applied to legacy designs and demands considerably lower test workload compared to existing approaches. Moreover, the scheme is robust and applicable to both digital and analog/mixed signal ICs.

The remainder of the paper is organized as follows: Section II describes related work with a focus on AF-based protection against counterfeit ICs. Section III presents the P-Val implementation details. Section IV describes the methodology and operation of P-Val. Section V presents security analysis as well as overhead results. Section VI concludes the paper.

II. Related Work

Due to the inadequacy of the existing industry level standard test/validation based reactive countermeasures [1], [4], several proactive DfS approaches have emerged. They include on-chip aging sensors [10], chip tracking schemes based on watermarking [11], IC fingerprinting and physical unclonable functions (PUF) [12], [13]. Aging sensors can however work only for isolating recycled/used chips. Moreover, they typically incur design and test efforts as well as area/power overhead, especially in small-scale chips [4]. Due to requirement of design modifications, aging sensors typically are inapplicable to legacy designs. The on-chip ring-oscillator (RO) based aging sensors [14] may only succeed in detecting recycled ICs if they have been used for a particular minimum usage time due to their low sensitivity under process variations. For cloned chips, watermarking, fingerprint and obfuscation based approaches typically incur significant design modifications. PUFs, on the other hand, exploit intrinsic random variations in the manufacturing process to generate unique identifier for each chip. However they are not applicable for detecting recycled chips without additional design protocols. Most PUFs incur considerable design effort, hardware overhead, test workload and cannot be applied to legacy designs. With analog ICs usually fabricated at older process nodes, PUFs are usually not applicable to them. Moreover, for authentication, some PUF implementations exhibit robustness issues due to temperature, voltage fluctuations etc. Hardware metering [15] can provide active defense against cloning attacks. However, they require the presence of an on chip random number block to generate a key for unlocking, resulting in die area overhead. The proposed security approach, "P-Val" presents a simple robust defense scheme against both recycling and cloning attacks at minimal package level overhead, offering similar protection as alternative approaches.

TABLE I
Comparison with existing AF-based anti-counterfeiting solutions

	Approach 1 [14]	***Approach 2 [16]***	***Proposed Approach***
Scope	Digital IC, no legacy design	Digital IC, no legacy design	All ICs & legacy designs
Design Mod. & Overhead	Yes (die level)	Yes (die level)	No (pkg. level)
Manufacturability	CMOS compatible	CMOS compatible	Complexity in BGA pkg.
Counterfeit Type (Security Level)	Aged (high) -	Aged (high) cloned (low)	Aged (high) cloned (high)
Perf. Overhead	None	Negligible	Minimal

The major differences of P-Val from existing AF-based anti-counterfeiting approaches are listed in Table I. Although the chip level AF based approach in [14] alleviates the problem of reduced sensitivity of RO based aging sensors, AF arrays with charge pumps, counters, multiplexers etc. on die would incur significant design modifications and area/power overhead. It is inapplicable to legacy designs and may not be feasible to implement it on all IC types. Although such an approach would estimate the chip usage statistics, often it is sufficient for a user to detect any sort of past tamper/handling of the IC to discard it, as is enabled by the P-Val. Moreover, the method in [14] is not applicable to cloned chips.

Besides [14], a mechanism for active defense against recycling and cloning using AFs and an OTP key was proposed by the authors in [16]. Although it allows easier manufacturability (CMOS compatible) as compared to P-Val implementation in some complex chip scale packages, it suffers from two major disadvantages : (1) it is a die-level approach which requires design modifications and incurs die-area overhead; (2) it uses one common key for all ICs of the same family, which is vulnerable to break-one-break-all type of cloning attacks. Conversely, P-Val provides a package-level defense which does not require any design modification and incurs no die-area overhead. It creates IC-specific signature based on intrinsic random variations, similar to that in PUFs and hence provides higher security against cloning attacks.

III. P-Val Implementation

Both the complementary security schemes of P-Val involve integration of an antifuse (AF) and test fuse (TF) to the corresponding pins at the package level. For protection against recycling, the AFs are left un-programmed where as for

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

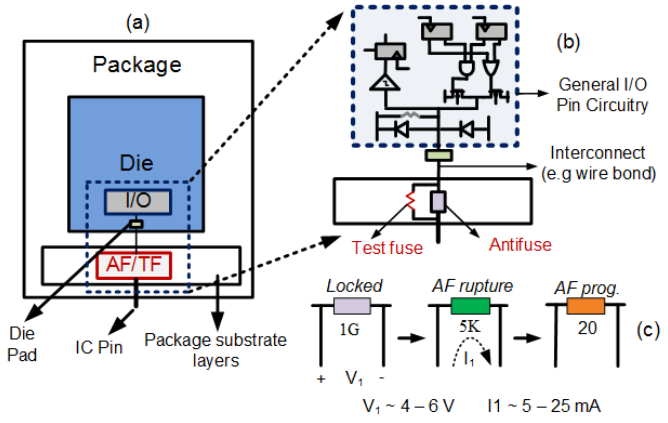

Fig. 4. a) AF/TF integration in packaging layers; b) interface of pin level AF/TF with I/O circuitry; c) steps in programming an antifuse.

defense against different cloning attacks, the desired set of AFs are programmed before deployment. For all the candidate pins, post-package testing is performed through the test fuses (TF), implemented in parallel to the AF. TFs are programmed before deployment. Fig. 4(a) and (b) illustrates a schematic of the package level implementation of the AF/TF based security scheme and its interface with the general I/O port logic. Before going on to the P-Val implementation details, we give a brief background on the major security component, the antifuse (AF) and its important properties that we have utilized in the P-Val scheme. We touch upon test-e-fuses (TF) as well.

A. Background Information on AF & TF

AFs are one time programmable (OTP) elements, behaving as a normally open switch (resistance $\sim 100M\Omega - 1G\Omega$) [6]. Once the desired programming voltage is applied across the terminals (mostly independent of polarity), irreversible changes occur in the structure of the AF. Consequently, applying a programming current leads to the formation of a conductive filament due to high joule heating and reaction between electrode and insulator material, hence behaving as a closed switch (resistance $\sim 10\Omega - 100\Omega$) [5], as shown in Fig. 4(c). AFs have been employed in secure, reliable programmable read-only memory (PROM) and military grade FPGA [5]. AFs are primarily of two different structures: a) PolySi-ONO-Diffusion and b) Metal-Insulator-Metal (MIM) structure. The latter provides greater ease of implementation in present micro-scale devices at desired electrical properties. Some of the specific MIM AF properties that are used in implementing P-Val are:

Property 1: The ON state resistance R_{on} is approximately inversely proportional to program current I_{pp} [7]. The median value of the MIM AF program resistances [8], [7] in the ranges of programming current within the maximum pin operating currents of different ICs between $15 - 40$ mA [17], [18], [19], is given by [7]:

$$R_{on} = \rho_{s,on}/(\Pi * rc) + \rho_{c,on}/(\Pi * rc) + (\rho_{c,on} * d)/(\Pi * rc^2) \quad \ldots\ldots(1)$$
$$where \quad rc = (I_{pp} * V_{f,p})/(4 * k_{eff} * (T_{co} - T_a))$$

In the above formula derived from electro-thermal models, $\rho_{s,on}, \rho_{c,on}$ are the electrical spreading and core resistivity under operation, d is insulator thickness, *rc* is core/filament radius, I_{pp} is program current, $V_{f,p}$ is programming fuse voltage, k_{eff} is equivalent AF thermal conductivity, T_{co} is core equilibrium reaction temperature and T_a is ambient temperature. Usually, equation (1) is simplified to incorporate the AF electrical, thermal conductivities and the core reaction temperature into a term V_f, called the characteristic fuse voltage [7], which is only dependent on the type of AF (Poly-Si or MIM). From the formula, it is evident that lower program currents lead to higher AF resistance and vice versa.

Property 2: Lower program currents lead to greater variation in the AF program resistance and vice versa [8]. At lower AF program currents, the effect of the insulator thickness and hence the conducting channel (instead of only a spherical core) is prominent (third term of R_{on} in equation 1).

Property 3: For programmed AFs, a read/operating current (I_{read}) below the program current I_{pp} leads to no AF structural alterations and hence consistent resistance values [8], [7]. However on I_{read} exceeding I_{pp}, the resistance decreases (to new value corresponding to I_{read}) due to greater joule heating and hence increased filament/core size [7]).

On the other hand, test-e-fuses (TFs) functionally represent the inverse of AFs i.e. normally closed switch ($\sim 20\Omega - 40\Omega$) [20] and blown open after programming. TFs are used for data security in FPGA, memory redundancy, chip identification, built-in self test etc [21]. They are programmed by passing a program current (e.g. $\sim 15 - 25mA$), causing chemical/structural changes due to metal electromigration at the electrodes and hence a resistance in the order of $M\Omega$s. A common TF incorporates metal silicide based structures.

B. P-Val Components

1) Effect of AF/TF on Normal Pin Operation: AF/TFs are incorporated into all/some of the the general purpose input output (GPIO) or output only pins of the IC. This allows programming of both components (AF-TF) by setting/writing

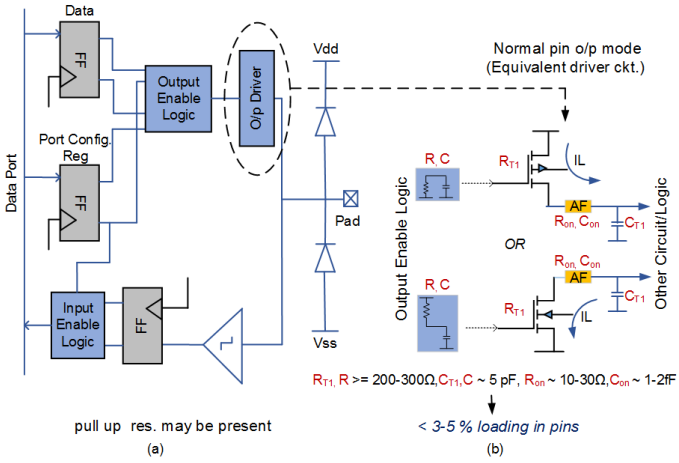

Fig. 5. a) A general representation of the I/O port circuitry found in different chips (μC, FPGA, μP etc.); b) minimal loading effect due to proposed scheme during the critical output mode operation of each candidate pin.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

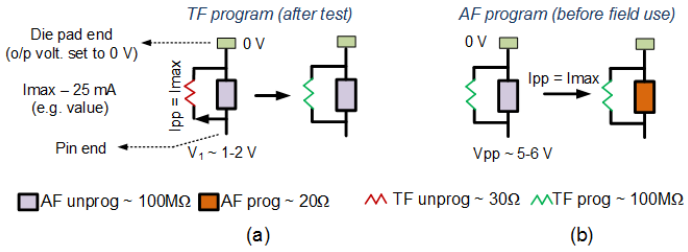

Fig. 6. Programming of (a) TF after post-package test by IC designer; (b) lock AF prior to field usage by system integrator in the pin output mode.

a particular output voltage at the pad (e.g. 0 V) and applying an external pin voltage equivalent to the program voltage and consequent passage of the AF/TF program current. A general representation of a GPIO port logic, found in slightly varying implementations in different types of chips such as microcontrollers, FPGAs, processors [17], [18], [19], [22] etc. is illustrated in the schematic in Fig. 5(a). Particular registers control the GPIO port configuration i.e. input or output (based on custom logic) as well as the port value/content. The electrical parameters of both AFs and TFs at the candidate pins have to be set to minimize any loading effects at the pin. The capacitance of both AF and TFs are of the order of $fF/\mu m^2$ [8], [9], [23] and hence minimal for typical dimensions, as compared to the usual total existing I/O capacitances in range of $\sim 5-10$ pFs [18], [19]. Moreover, the GPIO input resistance is of the order of $M\Omega$s and above, and hence a programmed AF during normal operation or an un-programmed TF during test would not cause any loading effects during input operations. The un-programmed and programmed resistances of an AF and TF are of the order of hundreds of $M\Omega$s and thereby does not hamper any electrical operations during post-package test (through TF) or in field (through AF) respectively. Hence the loading effects, in terms of logic propagation delay or load drive strength (due to programmed AF/un-programmed TF) should be analyzed in the critical pin output mode during normal/test operations.

In the output mode during normal operation, the port driver circuit reduces to an equivalent pull up/down transistor with a programmed AF in series (programmed TF in $M\Omega$s and hence considered open), as shown in Fig. 5(b). With the I/O supply voltages typically varying between 1.8-5 V and the maximum pin source/sink current between 10-40 mA across different grades and types of chips [17], [18], [19], [22] (referred chips vary between 180 nm to 32 nm in the process technology node), the ON resistance of the equivalent driver transistor is mostly $>= 200\Omega$. The resistances of the equivalent transistors, comprising the port enable logic are usually in the same range or higher as compared to drivers. Hence, the AF programmed resistance should be set accordingly to a low value to minimize the loading during the output mode. Minimization of loading effects also involves selecting the IC pins to be utilized for locking and authentication as described in the next section.

2) Antifuse (AF) Selection: For the P-Val scheme, we select Metal-Insulator-Metal (MIM) AFs due to their inherent advantages of low on-state resistance and capacitance, possible use of existing metal layers in manufacturing, lower breakdown voltages and high reliability [6]. The metal electrodes may be composed of Al, Cu, TiW etc [7], [24]. whereas the choice of insulators include Si_xN_y, SiO_2, amorphous Si, C etc [24], [23], [5], [8]. Although there exists CMOS compatible, transistor gate oxide breakdown based AF structures [25], we do not choose it as IC packages do not typically involve incorporation of silicon. For a chosen lower program voltage in the range of $\sim 4-6$ V, the AF insulator thickness would be ~ 20 nm [23], [26]. The program voltage would be applied externally at the pin (with pad at e.g. 0 V) to initiate a rupture or weak spot within the AF insulator link. The AF size is determined mostly by the electrode contact dimensions [27] and is within a maximum of 1-2 μm^2 [6], [9]. Possible pin choices for locking/authentication include most of the general purpose input-output (GPIO) or output only pins due to easier programmability, as illustrated in Fig. 6(b).

With respect to loading effects, critical pins such as high frequency chip clock/s (hundreds of MHz- GHz range), GPIO pins multiplexed with clock, oscillator input/outputs etc. are not selected to prevent any frequency degradation. Power pins are not chosen as stable functioning supplies are required for the TF and AF programming during chip unlock. Any pins with current limitations are also not considered. AFs in GPIO i/p mode (or input only pins) can also be carefully programmed in the input mode through forward biased protection diodes with proper choice of AF, diode, pull up/down resistance (if any) and pulse timing values such that the maximum operational ratings at the die pads are not violated. These are considered only in rare scenarios of too few candidate pins for P-Val. To minimize loading effects during normal operation, AF ON state resistance (R_{on}) is chosen between $10-30\Omega$ [8], [26], [24]. To enable this, according to the previously described MIM AF property 1, the final program current is chosen around the maximum pin current ranging typically from 10-40 mA across different IC types. In AF based FPGAs from Actel and Quicklogic, logic paths with even more than 5-10 MIM AFs in sequence can achieve a maximum frequency in the order of several MHz. As we are avoiding frequency critical pins in the order of hundreds of MHz to GHz, the chosen R_{on} values are guaranteed to minimize any loading. Multiple small program pulses could be used to further reduce AF program resistances [23]. The AF parameters are listed in Table II.

3) Test Fuse (TF) Selection: Programmed e-fuse resistances are of the order of 10-100 $M\Omega$. The common e-fuse structure incorporating a thin strip of Poly-Si, covered with

TABLE II
MAJOR PROPERTIES OF THE P-VAL MIM ANTIFUSE

Parameters	Value
Program voltage	4-6 V
Program current	10-40 mA ($\sim$ max. IC pin current)
Program duration	0.1-5 ms
OFF state resistance	$50M\Omega - 1G\Omega$
ON state resistance	$10\Omega - 30\Omega$
Size / dimensions	$< 1-2\mu m^2$
Insulator thickness	~ 20 nm

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

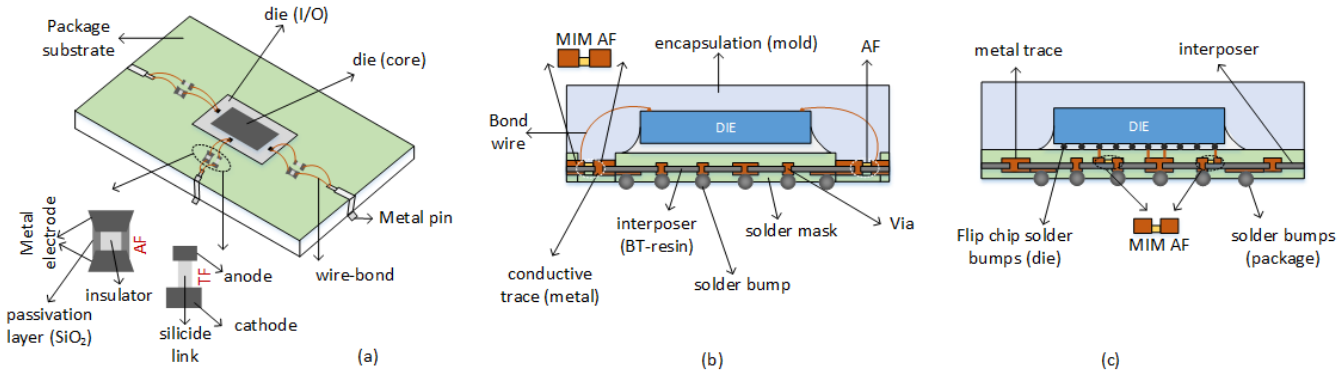

Fig. 7. (a) Discrete AF-TF integration in through hole and surface mount packages like QFN, QFP, PLCC, SSOP [30]; (b) P-Val implementation in wire bonded BGA based CSPs and (c) flip-chip bonded BGA based CSPs [28].

a thin silicide layer (e.g. $CoSi_2$, WSi_2) would be implemented [20], [21]. Programming involves electromigration of the metal atoms of the silicide due to localized heat generated from passage of programming current through the fuse link. Like AF, the size of the e-fuse is limited within $1-2\mu m^2$ [20]. The e-fuse properties are chosen such that the ON resistances are within $\sim 30\Omega$ [21] to minimize any loading effects during test. Their program properties should be selected according to the maximum operational ratings of the corresponding pins, thereby providing full IC test coverage at both wafer and assembly levels. A TF program scenario is shown in Fig. 6(a). Here, 25 mA program current at 2-3 V is representative of example e-fuse electrical ratings, which would be sufficient for full test coverage of many ICs like low voltage microcontrollers [17]. Desired fuse maximum current, associated voltage ratings as well as low ON-state resistances may be set by selecting appropriate e-fuse silicide materials, geometry, electrodes etc.

4) Package Level Fabrication: The AF-TF structures would be implemented at the package level, leaving the die untouched. P-Val can be implemented on all packaging types including current state of the art Ball Grid Array (BGA) based chip scale packages (CSP). Based on the chip mount (on for example a PCB), density of pins and package dimensions, IC packages are mostly categorized into 3 main types: 1) Through Hole; 2) Surface Mount and 3) Chip Scale Packages [28], [29], [30]. AF-TF structures would be integrated between the corresponding die pads and pins. Based on the package size with respect to the bare die estate and the type of existing connections between die pad and external pins, these units (AF-TF) would be implemented in discrete form on packaging substrate or grown on it selectively. With respect to these considerations, one can classify IC packaging technologies into 2 major categories: 1) through hole and most surface mount types (e.g. SSOP, QFP, QFN, PLCC) [29] where pads are connected to pin leads (at package substrate periphery) through normal wirebonds, afforded by the much greater package size compared to die ($>$ 4-5X); 2) chip scale packages where the package size is only $\sim$ 1.2X that of the die and pads are connected to external solder bumps by short wirebonds and substrate inter-layer traces (wire-bonded BGA) or through flip chip bonds (flip chip BGA) [28].

In the former scenario, due to much greater pad-pin spacings, the wirebonds are between 3-5 mm in total length [31], [32]. This allows enough package substrate area to integrate individual discrete AF and TF, of maximum sizes in the order of a few μm^2 (defined mostly by the sizes of the contacts $2\lambda X 2\lambda$ [27]) between the die pad and corresponding pin. The individual AF-TFs would be held in place by a material similar to the epoxy based die attach for mounting ICs on the packaging substrate [30]. As the sole additional packaging effort, wirebonds would be attached from the die pad to one of the AF and TF electrodes and from the other electrode contacts to the corresponding metal pin or leads, as illustrated in Fig. 7(a). In these cases, P-Val incurs only greater number of wire-bonds per candidate pin and usually no additional package area. Hence the extra cost is minimal. The wirebond diameters may have to be reduced from 1-1.2 mils to 0.5-0.7 mils to ensure a proper contact with the AF-TF cathode/anodes [32]. This scenario incorporates P-Val implementation in most of the IC types, especially the low and mid range chips. On the other hand, the special chip scale packages (CSP) for high end processors, system-on-chips, DSPs etc. would involve controlled fabrication of the AF, TFs on the packaging substrate mostly by reactive sputtering techniques [33], [34]. The metal layers from the package substrate conductive traces (e.g. Cu, Al) can be utilized to serve as the electrodes where as the AF insulator layer of for example Si_xN_y and Poly-Si and silicide (e.g. WSi_2) of e-fuse can be deposited selectively using masks. Schematics of P-Val implementation in CSPs are illustrated in Fig. 7(b) and (c). Here, only the AFs are depicted in the package cross section view. The TF layers would be fabricated and integrated in a similar manner. Fig. 7(b) and (c) only depict one layer of interposer and conductive trace in the package. Many CSPs contain multiple such layers between die pad and external solder bumps [28]. In these scenarios, the same method of AF-TF fabrication can be performed on the top stack layer. Through the additive reactive sputtering, one does not need to deposit entire layers and perform chemical etch out to form structures, minimizing the net additional cost. Either of the two procedures (discrete AF/TF or deposition) may be implemented in wire-bonded BGA based CSPs.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

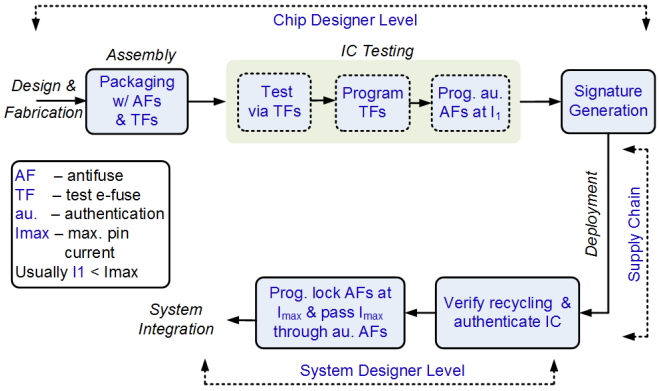

Fig. 8. Life-cycle of a legitimate IC with P-Val implementation.

IV. Pin Locking and IC Authentication

The flow (involving design and business cycle) of a legitimate chip with P-Val implementation is depicted in Fig. 8. P-Val unifies two novel complementary security approaches:

A. Pin Locking

Antifuses (AFs) inserted in few chip pins (from GPIO or output only port set) disables the pin functions and hence the term "pin locking". All ICs from a family would have the same pins locked. The number of locked pins could be one especially in small scale chips, but usually a few pins would be selected to significantly affect the IC functionality until the AFs are programmed.

At the level of the system designer/end retailer (trusted entities in model), a programming device (PD) could be securely exchanged by the chip manufacturer to accelerate the verification, unlock and authentication process, at the expense of slight increase in cost. This device would integrate the voltage pulser, current regulator, the locked pin locations for the IC family and verification logic for the pin lock/unlock condition (along with signature calculation). It is assumed trustworthy, tamper proof and exchanged securely in the P-Val implementation. A PD is not a necessity for the P-Val scheme, but helps in easier adoption of the proposed approach by system designers with respect to test effort and time-to-market constraints. Besides, a PD would help in standardizing the AF resistance measuring process for authentication and avoid any site-to-site variation on measurement accuracy. With a PD or own set up, the system designer verifies the lock/unlock condition by measuring the order/range of lock pin resistances in the port o/p modes (by measuring current under applied pin voltage) and/or checking the chip functional outputs and proceeds with programming the AFs in case of a new IC. As the AFs are one-time-programmable (OTP) due to irreversible chemical/structural alterations during program, P-Val provides robust, active defence against recycled ICs.

B. IC Authentication Methodology

The random intrinsic variation of AF programmed resistances around nominal value (for same program parameters) can be utilized to create chip-specific signatures for authentication. The manufacturing and programming process induces variation in device parameters such as insulator thickness, electrode surface roughness, core radius etc. To the best of our knowledge, AF program resistance variation have only been studied [8], [9], [24], [26] to ensure that their values are constrained within a threshold (e.g. 50-100 Ω for MIM AF) to satisfy critical path delays in FPGA applications. Here, we aim to utilize the inherent variations to our benefit for authentication, similar to PUFs using random process variations in device/circuit parameters [12].

The sources of these variations could be manifold, as inferred from studies regarding conducting filament characteristics, core temperature boundary, link material analysis etc. [7], [23], [8]. Possible sources such as insulator thickness, side wall geometry, AF electrical and thermal properties, filament stoichiometry (not all independent) etc. are illustrated in a representative programmed AF cross section schematic in Fig. 9(a). The variation of AF program resistances (R_{on}) between 20 and 30 Ω, for a program current (I_{pp}) of 20 mA is illustrated in the probability density function (pdf) in Fig. 9(b) (differentiation of empirical cumulative distribution in [8]).

Corresponding to AF properties 1 and 2 mentioned in Section III, higher variation and median value of R_{on} for lower I_{pp} are illustrated in Fig. 9(c) for fabricated MIM AFs [8]. The greater variation can be utilized for enhanced uniqueness of the signature space. For a MIM AF program voltage around 4-6 V, the minimum I_{pp} utilized for forming the conductive filament is $\sim$ 5 mA [8], [23]. In this case, R_{on} would range from 50 Ω to $\sim$ 80Ω [8]. Utilizing this large typically random variation, the individual programmed authentication AF resistances would be measured after chip testing and the IC signature generated according to the protocol described in the ensuing section. AF property 3 prohibits an AF operating current beyond I_{pp} for invariant AF program resistances and thus robust signatures. For this purpose, test e-Fuses (TF) of low resistance and program current around max. pin current would also be in parallel to the authentication AFs for full test coverage. After test, TFs are blown and AFs programmed.

After authentication, along with programming the lock

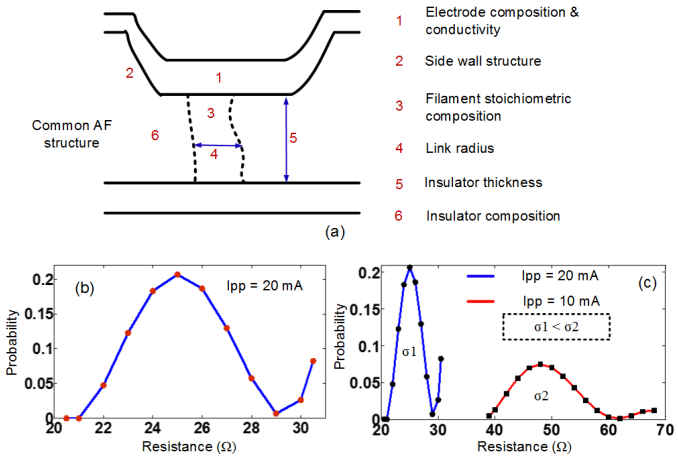

Fig. 9. (a) Possible sources of intrinsic variation of programmed AF resistances (R_{on}); (b) Variation of R_{on} of MIM AF with amorphous Si insulator at 20 mA program current (I_{pp}) [8]; (c) Greater variation of AF R_{on} at lower I_{pp} at similar program voltages, duration and pulse patterns [8].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

AFs at I_{max}, the system designer passes I_{max} through the authentication AFs as well (shown in Fig. 8), where I_{max} is $\sim$ 15-40 mA across types and families of ICs. According to AF Property 3, this would reduce R_{on} of all AFs to between $10 - 30\Omega$ [8], [26], [24], which is guaranteed to minimize any loading effects during normal field operation. Hence in P-Val, MIM AF properties are suitably utilized to create unique signatures for authentication as well as minimize any loading effects at the pins in field. In P-Val, we do not consider the authentication beyond system implementation i.e. in-field. Hence, to minimize any performance overhead, the AF R_{on} were all intentionally reduced after successful verification.

One point to note here is that after authentication AFs are programmed, along with satisfying the condition of $I_{read} < I_{pp}$, the measured AF resistance slightly depends on the I_{read} value because of self heating effects [7], [8]. Hence the current at which the resistances are measured for both signature creation (IC designer) and verification (system designer) should be approximately the same and close to, but less than I_{pp} for the different pin AFs. These measurement conditions may be stored in the manufacturer's database and/or programming device if any. All the legitimate IC signatures are stored in the manufacture's database. When an IC reaches a trusted entity, he/she generates the chip signature after measurement. Consequently, it is compared with the signatures stored in the database to verify a match and hence considered a legitimate IC. During signature creation and verification, AF R_{on} are measured by setting the corresponding pad at a fixed voltage (e.g. 0 V) and applying a measuring potential at pin to pass I_{read}. The ratio of applied voltage to I_{read} gives AF R_{on}.

C. Signature Generation

The chip specific signature is created and stored at the final stage prior to deployment. The steps of the signature generation protocol are depicted below:

Signature Generation (same I_{pp} for all AFs)

Input: $[R_i]$, the resistance vector of chip,
for all $i \subseteq (1, .., M)$, M←no. of auth. pins

Initialization: C ← 0

for all $i \subseteq (1, .., M-1)$,
for all $j \subseteq (i+1, .., M)$,
C ← C + 1

Comparison: If $R_i >= R_j$ (normalized due to same I_{pp})
$P_s[C]$ = 1
else
$P_s[C]$ = 0
end
end

Output: Sig = $[P_s[k]]$ for all $k \subseteq (1, .., MC_2)$

The inputs to the chip signature generation algorithm are the measured program resistances of the authentication pin AFs. As AFs in a chip are typically programmed at the same I_{pp} (same mean value of distribution), a simple comparison based scheme is utilized to create robust signatures (values already normalized). Any two authentication AF R_{on}, chosen in a predetermined sequence for all chips, are compared to create a 1 or 0 signature bit. This method also utilizes the full entropy of the signature space. Another significant advantage of the comparison based scheme is the robustness to any common-mode variations of AF R_{on} with temperature, which might occur before/during measurement. Although much smaller than metal interconnects [23], [8], programmed MIM AF resistances exhibit a non-negligible positive linear temperature coefficient in the order of $(4 * 10^{-4}) - (8 * 10^{-4})K^{-1}$ at 298 K, in the P-Val current ranges and vary linearly according to $R_T = R_0[1 + \beta(T - T_0)]$ [8]. Here, R_T is the AF resistance at temperature T K and R_0, β are the resistance and electrical resistivity at a reference temperature T_0. For example, for $I_{pp} = 10mA$, the MIM AF R_{on} increases by a maximum of 4% from $25^\circ - 80^\circ$. Our comparison based signature generation automatically makes P-Val robust against the effect of these typically linear temperature variations. We do not analyze temperature lower than 25° as AF resistances are mostly unaltered with decreasing temperatures [8].

As compared to global normalization and digitization based algorithms, where all chips are compared amongst each other, normalized with respect to globally chosen mean, minima etc. and possibly digitized, the proposed inter-pin (same chip) comparison scheme provides the following advantages: 1) Robustness to temperature based R_{on} changes and AF fabrication related common biases if any; 2) Utilizing the full entropy of the signature space to create unique, robust signatures; 3) No requirement of measurement or storage of any global pin value like mean, median etc. of R_{on} by the chip manufacturer. With the proposed signature scheme, even 20 AF pins would lead to $20C_2 = 190$ candidate signature bits. This allows proper selection of bits to create a robust 128 bit signature and also minimize any bit correlations during comparison.

V. Security Analysis

As the counterfeiting of ICs is such a lucrative malpractice in terms of economic benefits, adversaries would try do everything possible to defeat any protection scheme. In the next subsections, P-Val is analyzed from different angles in how an attacker may attempt to bypass its security features and at the same time maintain an economic benefit, which is the main purpose of counterfeiting.

A. Security of P-Val against recycled chips

Antifuses (AFs) are one-time programmable (OTP) due to formation of an irreversible conductive filament on programming due to chemical reaction between the insulator and the metal electrodes. The different recycled IC based attack channels on proposed scheme and the corresponding P-Val defenses are illustrated in Fig. 10. As AFs are OTP, the sole viable way an attacker can attempt to bypass P-Val for an used chip is to de-package the IC, replace the programmed AFs (previously locked) with new ones and then re-package and insert into supply chain. In P-Val, the position

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

of the locked and authentication pins are transparent. With state of the art tools, an adversary can de-package, replace components and re-package without detection by physical and microscopic analysis tools. However from the economic perspective, as compared to first time integration, replacing AF-TFs without leaving any functional/electrical detection traces is prohibitively more expensive. To elaborate, by far, the most common practice that is followed by attackers for recycling is to scrape off the used ICs from the system level boards, fix any wear and tear in the pin/s and physical defects on the external package, remark the surface if required and insert them back into the supply chain. This incurs minimal cost. Minimal pitch surface mount and chip scale packages (flip chip and wire-bonded BGA), where the AF-TFs are fabricated on the packaging stack makes their replacement significantly more difficult due to complexity in handling of narrow traces, solder balls, micro-via, interposer layers etc. To replace the programmed package level lock AF, an attacker would require the access to the state of the art micro-electronic tools/resources. More importantly, dealing invasively with the package increases the chances of enhanced contact capacitance, incorrect alignments, micro-via alterations, pad wearing etc.. These may get detected by system designer via IC parametric tests like maximum frequency, drive current, burn in and high speed functional tests. Hence, the economic gains from recycling reduces significantly when one has to expend significant time and resources to evade detection.

Even if we assume that an attacker successfully does the replacement of the lock pin AFs, the IC would fail at the authentication stage as the programmed ON-state resistances of all the authentication AFs had been reduced irreversibly (from values used to create signature) prior to in-field usage (by program at max. pin current) and hence no resulting signature match. Even in an extreme scenario, if the adversary replaces all the lock as well as authentication pin AFs and programs the latter set after reverse-engineering, differences in fabrication, program parameters coupled with intrinsic random variations would lead to unique cloned IC signatures. As these will not be stored in the IC manufacturer's database, the corresponding chips would be detected as cloned ICs. Detection of any type of counterfeit ICs (recycled as clone or vice versa) suffices to prevent them from further usage in electronic systems, which is the main goal of security schemes.

B. Security of P-Val against cloned chips

In this subsection, through theoretical analysis, mathematical formulation and simulation based results, we analyze the security provided by P-Val against different forms of cloning attacks. Fig. 2(b) had illustrated the different types of cloning threats like piracy of IP, overproduction of ICs as well as reverse engineering after fabrication. With P-Val implementation, along with these attacks, an IC signature need to match one in the database to successfully pass the authentication phase. Due to complexity of implementation involving different entities in semiconductor business model, the verification of a particular signature (hence a chip) in the IC manufacturer's database does not lead to any database

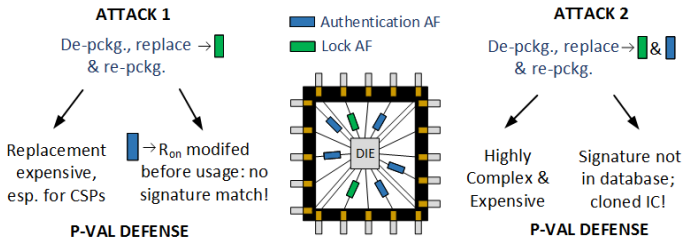

Fig. 10. Security provided by P-Val against different attempts by an adversary to bypass the used/recycled chip detection scheme.

update (to note its verification once) in the P-Val scheme. Hence, any chip having a signature matching any legitimate verified IC would also be authenticated in P-Val. As a result, an adversary attempts to reproduce the signatures of legitimate chips in his manufactured cloned ICs. Hard-coding the signature bits in a non-volatile memory is not possible as P-Val requires resistance measurements and off-line generation of signatures. If programming devices are used, we assume their secure exchange and tamper protection. To pass the P-Val authentication scheme, an attacker, assuming the role of a system designer, can buy a few legitimate chips and generate their signatures. Consequently, he/she would attempt to copy these signatures with highest probability.

Referring to the signature generation algorithm, it is sufficient for an adversary to copy the relative values of the AF resistances (compared to actual magnitudes) of a legitimate chip. Similar to the principles of PUF, random intrinsic variations in the program AF resistances arise from different inherent structural, chemical and programming characteristics, which are not controllable [7], [8], [9]. As a result, for better controllability and thereby enhancing the match probability, an adversary might attempt to replicate signatures of legitimate chip/s by inserting *chip-scale precision resistances* (tight distribution) of corresponding relative values in cloned ICs.

1) Precision Resistance Insertion: To obtain a set of resistance values with high probability, an adversary would wish to use a resistance type with much tighter distribution than AFs, along with a miniature form factor to be integrated into the IC package. Flat chip scale thin film precision resistors with a tolerance of $\sim 0.1\%$ are used in some electronic applications [35], [36]. In a cloning scenario, the adversary integrates precision resistors of the measured relative magnitudes.

This attempt can be defeated if we can detect whether the measured authentication resistance originates from a programmed AF or any other material such as precision resistors, test-fuse etc. Some unique property characterizing programmed AFs needs to be used as an additional defense layer e.g. the aforementioned property 3 of the MIM AFs can be utilized i.e. if $I_{read} > I_{pp}$, the AF ON-state resistance (R_{on}) reduces due to enlarged filament size. In P-Val, AFs are programmed at $I < I_{max}$ to enhance intrinsic variation, and consequently programmed at I_{max} to minimize R_{on} and hence any loading effects in-field. Normal chip scale precision resistors or test-fuses etc. do not exhibit this unique property. Hence, the reduction of resistance on final program roughly according to empirical equations proves that the resistance

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

measured is due to a programmed MIM AF and thus detects an adversary malice of the type mentioned. Other distinct AF properties could be used for verification as well. These would be verified only in the scenario of a signature match.

2) AF Integration in Cloned ICs: For cloning, an attacker could integrate AFs at the respective pin positions of the chip and program them. As AFs of different possible materials, geometries and program properties all suffer from intrinsic manufacturing/program related variations, the success of an adversary i.e. cloned IC matching any original chip signature is probabilistic. The probability of cloning a small scale or low end chip (e.g. some μCs, analog ICs) with less number of pins is higher as the signature space (NC_2 bits) is typically exponentially dependent on the number of pins. Different chosen AF distributions (different structure, chemical composition, program voltage etc.) might lead to varied adversary success rates. In the next section, we calculate the minimum number of authentication pins to statistically minimize this cloning probability. For ease of calculations, we favorably assume (from attacker's point) that the legitimate and cloned IC AF distributions are the same, which the attacker could achieve by using the same fabrication facility etc.

Minimum number of Authentication Pins: If there are "N" authentication pins and each AF program resistance is represented by X_i, then with "M" total existing legitimate ICs, the probability P_r of a cloned IC matching any legitimate chip signature can be theoretically formulated as:

$$P_r = P((X_1, X_2, ..., X_{N-1}, X_N) \subseteq (O_1 \bigcup O_2 \bigcup ..O_K))$$

where $O_1, O_2, ..., O_K$ constitute the regions in the total signature space (maximum of 2^{NC_2} bits) comprising of the "M" legitimate ICs. This is also conceptually depicted in the representative set diagram illustration in Fig. 11(a). As estimating this probability from theoretical formulation considering all possible scenarios is extremely complex, we statistically estimate the probability through simulation studies considering the cumulative distribution function (cdf) of AF R_{on} in [8] (Fig. 11(b) upper). Although the AF composition in P-Val is a bit different from that in [8], the simulation results serve only to estimate representative values for the cloning probability. We perform the analysis for $I_{pp} = 10mA$ (lowest empirically analyzed value in [8]).

Simulation Setup & Results: The probability density function (pdf) of programmed AF resistances, derived from differentiation of cdf in [8]) is shown in Fig. 11(b) (lower). The number of authentication pins are varied from 8 to 16. We considered 1 million legitimate chips. For each chip, assuming the same I_{pp} for all AFs, programmed resistance (R_{on}) values are chosen randomly according to the pdf and the signature calculated following the protocol. The resolution of the measurement determines the the total number of possible resistance values of a programmed AF. It is derived from the specification of a simple, low cost multi-meter as $\sim 0.05\Omega$ or $50m\Omega$ [37]. For a representative cloned IC, AF R_{on} values corresponding to the number of authentication pins are randomly selected from pdf and the signature calculated. For

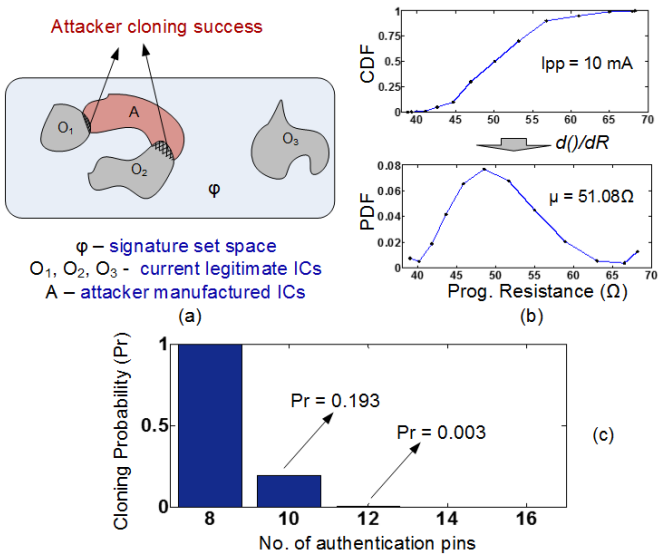

Fig. 11. (a) Example set diagram representation of match probability of cloned IC signatures. (b) CDF and derived PDF at I_{pp} of 10 mA used for simulation studies; (c) Variation of calculated cloning probability with number of authentication pins (1 million legitimate ICs).

10000 such iterations (from simulation time constraints), the calculated signature is compared with all the legitimate signatures for a match. One or more matches leads to increment of a counter by 1 for every iteration. The ratio of the final counter value to 10000 is an estimate of the cloning probability of a legitimate IC. All simulations are performed in Matlab.

The variation of calculated cloning probability with the number of authentication pins is illustrated in Fig. 11(c). As observed, considering 1 million legitimate ICs of a certain type, there will always be a match up to 8 authentication pins. For 500,000 original chips, the corresponding probability reduces to 0.91. However due to the exponentially increasing signature space, this probability reduces drastically to 0.19 for 10 pins and 0.003 for 12 pins. This suggests that on an average, with 10 authentication pins, an attacker has to fabricate 100 chips for 19 to pass P-Val and hence not economically viable. No match was found with greater than 12 pins. Hence a chip with P-Val and minimum ~ 10 authentication pins would be typically secure against different cloning attacks. This would include majority of the IC types/families in the market.

C. Protection against Overproduced ICs

One prevalent form of counterfeiting is overproduction of chips by a malicious foundry beyond the contract with the IC designer. As the AF-TF fabrication process is the same for legitimate and overproduced chips in this case, there is a much higher probability of complete resistance distribution match although AF programming happens under the control of the designer. Even then, as described previously, due to intrinsic random variations, IC signatures with 10 or more authentication AFs would be either impossible to clone or copying is mostly not an economically viable option. This includes usage scenarios of attackers modifying the packaging of the overproduced lot to enhance the probability of signature overlap with legitimate, as discussed in last section with chip

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

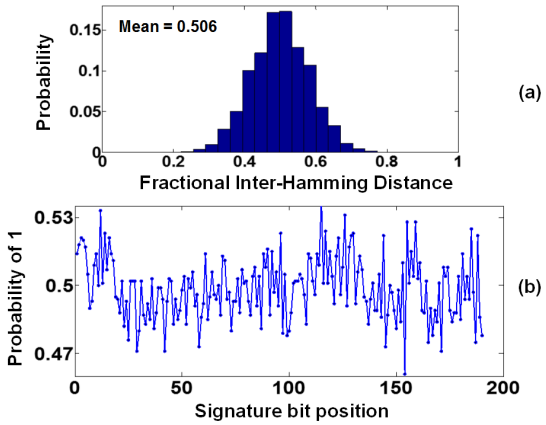

Fig. 12. (a) Distribution of fractional Inter-Hamming distance for 190 bit signatures in 1000 chips at $I_{pp} = 10mA$; (b) Probability of bits being 1.

scale precision resistors. In P-Val, the signatures are generated at the end of the IC design cycle, just before deployment. As overproduced chips follow an alternate parallel route to the supply chain, the corresponding unique signatures would be never stored in the original manufacturer's database. Hence they would be easily detected by a trusted party.

D. Uniqueness and Robustness of Signature

Uniqueness and robustness of signatures is important for reliably authenticating each chip from the IC manufacturer.

1) Simulation Setup & Metrics: Signatures are analyzed for 1000 legitimate chips and 20 authentication pins per chip. The MIM AF program resistances (R_{on}) are taken from the measurements in [8] as in previous section. With 20 pins, 190 ($20C_2$) bit IC signatures are generated. The metric quantifying the signature uniqueness [13] is the fractional Inter-Hamming distance distribution with average (HD_{inter}) as:

$$HD_{inter} = (2/(N*(N-1))) * \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} HD_{ij}$$

Here HD_{ij} is the fractional Inter-Hamming distance between chips i and j and N is the number of chips. HD_{inter} is desired to be close to 0.5. As discussed, P-Val is robust to temperature variations. During measurement, random instrumentation noises can be nullified by averaging over multiple iterations (as done in [8]) and hence not considered here. The robustness of P-Val is tested in an extreme scenario of resistances being measured only at resolutions between $0.5 - 1\Omega$, perhaps due to limitations of measurement setup or high noise levels. In this case, close resistance values could lead to bit flips during comparison. Signature robustness has been quantified by the fractional Intra-Hamming distance distribution [13] and its average value (HD_{intra}) is:

$$HD_{intra} = (2/(N*Z*(Z-1)))) * \sum_{i=1}^{N} \sum_{j=1}^{Z-1} \sum_{k=j+1}^{Z} HDI_{ijk}$$

Here HDI_{ijk} is the fractional Intra-Hamming distance for chip i between the j^{th} and k^{th} measurements. Here Z = 10 i.e. 10 measurements. HD_{intra} should be ideally zero.

2) Results: Fig. 12(a) illustrates the fractional Inter-Hamming distance distribution with 1000 chips. Majority of the values lie between 0.4 and 0.6 with the mean HD_{inter} = 0.506, signifying high uniqueness of signatures. The probability of each of the bits being 1 varies between 0.47 and 0.53 (shown in Fig. 12(b)), signifying absence of any 1/0 bias.

For comparison of the condition of measurement resolution between $0.5 - 1\Omega$ (10 values uniformly drawn in range) with the reference, the corresponding metric is illustrated in Fig. 13. Even in this scenario, most values are located within 0.05 with mean value 0.0242, which is acceptable for security primitives like PUFs [12], [13]. Hence P-Val leads to the generation of unique, robust chip signatures for authentication.

E. Sample Cloning and Overhead Values

The approximate number of candidate authentication pins in different IC types and the resulting clone probability according to simulation results is given in Table III. We have considered high end ICs like a Intel-i7, Xilinx Spartan-6, TMS320C620 DSP and mid, low range chips namely a μC (ATmega32L) and an analog multiplexer (ADG509F). For high end chips, with supply/GND comprising a large fraction of pins, only 10% of the total pins are considered here for authentication AFs. As evident from simulation results, high end chips with P-Val are impossible to clone. For the μC (40 pins), selecting even 20 out of the 32 GPIO ports would practically reduce the probability to zero. For the low end chip ADG509F (16 pins) all 10 I/O pins (select, input ports) would be considered for P-Val. With a resulting clone probability of ~ 0.2, the economic shift in cost/benefit ratio would prevent any cloning attempts.

With the area of MIM AF and TF structures being dominated by the size of the electrode contacts ($2\lambda X 2\lambda$), the package area overhead is negligible ($< 0.05\%$) for the different ICs (Table III), considering that each AF-TF pair requires overhead beyond package estate. P-Val incurs zero design modifications and die area overhead. All AFs are programmed at maximum pin currents post-verification, typically reducing R_{on} to $10 - 30\Omega$. Together with capacitances in fF range, loading effects on the pins are minimal. The only P-Val overhead would be a minor rise in packaging cost.

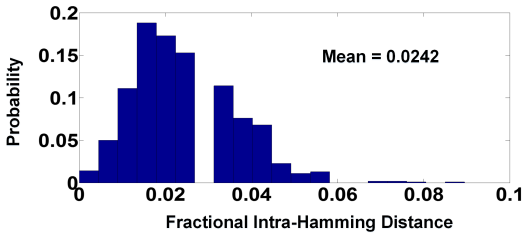

Fig. 13. (a) Fractional Intra-Hamming distance distributions for 190 bit signatures in 1000 chips with measurement resolution between $0.5 - 1\Omega$ and 10 measurement instances (compared with reference of 0.05Ω resolution).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCAD.2015.2501311, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems

TABLE III
SECURITY & ESTIMATED PACKAGE AREA OVERHEAD OF P-VAL

	No. of Authentication AFs	Approx. prob. of cloning 1 chip	Package Area Overhead (%)
Core-i7	135	~ 0	$4.2 * 10^{-4}$
Spartan 6-LX	118	~ 0	$5 * 10^{-4}$
TMS320C620	35	~ 0	$1.1 * 10^{-4}$
ATmega32(L)	20	~ 0	$4.4 * 10^{-2}$
ADG509F	10	~ 0.2	$1.6 * 10^{-2}$

VI. CONCLUSION

We have presented *P-Val*, a novel package-level protection against counterfeiting attacks, based on insertion of antifuse (AF) devices to select pins of an IC. It protects against both recycled and cloned ICs, which are the primary forms of counterfeit chips. Insertion of the one-time programmable AFs in few IC pins provide active defense against aged chips. On the other hand, protection against cloning attacks is achieved through programmed AF-based IC authentication process. It exploits inherent random variations in programmed resistance of AFs due to both manufacturing and programming process to create an unique signature per chip. To enable testing of pins with AFs, test e-Fuses (TFs) are inserted in parallel. TFs are programmed after package testing is completed.

Unlike existing active protection approaches against counterfeiting like PUFs, P-Val incurs no design modifications or die-area overhead and comes at lower test cost. Moreover, it can also be applied to legacy designs. Another important advantage of P-Val is that it is applicable to all classes of chips including analog and mixed-signal ones. Theoretical analysis and simulation results verify that with P-Val, it is practically infeasible to clone complex chips with high pin counts (e.g. processor, FPGA). For chips with smaller pin counts (e.g. 9-10 suitable pins), P-Val makes the cloning practice economically not viable for an adversary. Future work will include security analysis for different AF types and fabrication of IC packages with integrated AFs to experimentally validate P-Val.

REFERENCES

[1] U. Guin, M. Tehranipoor, D. DiMase & M. Megrdichian, "Counterfeit IC Detection and Challenges Ahead", *ACM SIGDA*, Mar 2013.
[2] "Counterfeit Chips on the Rise", *http://spectrum.ieee.org/computing/*.
[3] "Chip counterfeiting case exposes defense supply chain flaw", *http://www.eetimes.com/*.
[4] K. Huang, J. M. Carulli Jr. & Y. Makris, "Counterfeit Electronics: A Rising Threat in the Semiconductor Manufacturing Industry", *ITC*, 2013.
[5] S. Chiang et. al, "Antifuse Structure Comparison for Field Programmable Gate Arrays", *IEDM*, 1992.
[6] S. J. Wang et. al, "High-Performance Metal/Silicide Antifuse", *IEEE Electron Device Letters*, Vol. 13(9), 1992.
[7] G. Zhang et. al, "An Electro-Thermal Model for Metal-Oxide-Metal Antifuses", *IEEE Trans. Electron Devices*, Vol. 42(3), 1995.
[8] C-C. Shih et. al, "Characterization and Modeling of a Highly Reliable Metal-to-Metal Antifuse for High-Performance and High-Density Field-Programmable Gate Arrays", *Reliability Phy. Symp.*, 1997.
[9] S. S. Cohen et. al, "A Novel Metal-Insulator-Metal Structure for Field-Programmable Devices", *IEEE Trans. Electron Dev.*, Vol. 40(7), 1993.
[10] X. Zhang, N. Tuzzio & M. Tehranipoor, "Identification of Recovered ICs using Fingerprints from a Light-Weight On-Chip Sensor", *DAC*, 2012.
[11] A. B. Kahng et. al, "Robust IP Watermarking Methodologies for Physical Design", *DAC*, 1998.
[12] G. E. Suh & S. Devadas, "Physical unclonable functions for device authentication and secret key generation", *DAC*, 2007.
[13] A. Krishna, S. Narasimhan, X. Wang & S. Bhunia, "MECCA: A Robust Low-Overhead PUF using Embedded Memory Array", *CHES*, 2011.
[14] X. Zhang & M. Tehranipoor, "Design of On-Chip Lightweight Sensors for Effective Detection of Recycled IC", *IEEE Tran. on VLSI Systems*, Vol. 22(5), 2014.
[15] Y. M. Alkabani & F. Koushanfar, "Active Hardware Metering for Intellectual Property Protection and Security", *USENIX Security*, 2007.
[16] A. Basak, Y. Zheng & S. Bhunia, "Active Defense against Counterfeiting Attacks through Robust Antifuse-based On-Chip Locks", *VTS*, 2014.
[17] "PIC16F84A Data Sheet", *http://www.microchip.com/*.
[18] "8-bit AVR Microcontroller", *http://www.atmel.com/*.
[19] "Virtex-5 FPGA User Guide", *http://www.xilinx.com/*.
[20] C. Kothandaraman, S. K. Iyer & S. S. Iyer, "Electrically Programmable Fuse (eFUSE) Using Electromigration in Silicides", *IEEE Electron Device Letters*, Vol. 23(9), 2002.
[21] N. Robson et. al, "Electrically Programmable Fuse (eFUSE): From Memory Redundancy to Autonomic Chips", *CICC*, 2007.
[22] "Intel Core i7 Processor Family ", *http://www.intel.com/*.
[23] K. E. Gordon & R. J. Wong, "Conducting filament of the programmed metal electrode amorphous silicon antifuse", *IEDM*, 1999.
[24] Y. Tamura & H. Shinriki, "Most Promising Metal-to-Metal Antifuse based l0nm-thick p-SiNx film for High Density and High Speed FPGA Application", *IEDM*, 1994.
[25] J. Kim & K. Lee, "3-Transistor Antifuse OTP ROM Array using Standard CMOS Process", *Symposium on VLSl Circuits Digest of Technical Papers*, 2003.
[26] M. T. Takagi et. al., "A Highly Reliable Metal-to-Metal Antifuse for High-speed Field Programmable Gate Arrays", *IEDM*, 1993.
[27] "The Antifuse", *http://www10.edacafe.com/*.
[28] "Assembly and PCB Layout Guidelines for Chip- Scale Packages", *http://www.microsemi.com/*.
[29] S. Nimbal, "IC Packaging", *http://www.slideshare.net/*.
[30] S. L. Buedo, "Electronic Packaging Technologies", *http://www.slideshare.net/*.
[31] "Wire Bonding Services", *http://component-solutions.tek.com/*.
[32] "Packaging Options", *https://www.mosis.com/*.
[33] R. P. Howson, "The reactive sputtering of oxides and nitrides", *Journal of Pure and Appl. Chem.*, vol. 66(6), 1994.
[34] "BASIC CONCEPTS OF REACTIVE SPUTTERING", *http://reactive-sputtering.info/node/99*.
[35] "Precision Thin Film Chip Resistor", *http://www.vishay.com/*.
[36] "Thin Film", *http://www.mini-systemsinc.com/*.
[37] "Low-Cost 61/2-Digit Multimeters", *http://www.ni.com/*.