# PiRA: IC Authentication Utilizing Intrinsic Variations in Pin Resistance

Abhishek Basak, Fengchao Zhang and Swarup Bhunia
Department of EECS, Case Western Reserve University, Cleveland, OH-44106, USA
{axb594, fxz67, skb21}@case.edu

***Abstract*— The rapidly rising incidences of counterfeit Integrated Circuits (ICs) including cloning attacks pose a significant threat to the semiconductor industry. Conventional functional/structural testing are mostly ineffective to identify different forms of cloned ICs. On the other hand, existing design for security (DfS) measures are often not attractive due to additional design effort, hardware overhead and test cost. In this paper, we propose a novel robust IC authentication approach, referred to as *PiRA*, to validate the integrity of ICs in presence of cloning attacks. It exploits intrinsic random variations in pin resistances across ICs to create unique chip-specific signatures for authentication. Pin resistance is defined as the resistance looking into or out the pin according to set parameters and biasing conditions, measured by standard tests for IC defect/performance analysis such as input leakage, protection diode and output load current tests. A major advantage of PiRA over existing methodologies is that it incurs virtually zero design effort and overhead. Furthermore, unlike most authentication approaches, it works for all chip types including analog/mixed-signal ICs and can be applied to legacy designs. Theoretical analysis as well as experimental measurements with common digital and analog ICs verify the effectiveness of PiRA.**

## I. Introduction

A counterfeit Integrated Circuit (IC) can be a recycled die, cloned or copied design without lawful rights, an overproduced component, or a misrepresented, failed real part. Counterfeit ICs usually suffer from altered functionality, poor performance or degraded reliability of operation. The significant rise in counterfeit ICs in the semiconductor market is a major concern to chip designers, system integrators and end users in diverse industrial sectors including consumer electronics, automobile and networking [1], [2]. These chips encompass all types of ICs, including analog, mixed-signal and digital as illustrated in Fig. 1(a) [3]. Apart from defaming the original IC manufacturing companies and affecting their revenue, counterfeit ICs have serious implications in defense and mission critical applications, thus even jeopardizing national security. The global cost of counterfeiting and piracy is estimated to rise to ∼1.2 to 1.7 trillion dollars by 2015 [1].

The current semiconductor business model offers various sneak channels that can be exploited by an adversary to insert fake chips, as illustrated in Fig. 1(b). The two major categories of counterfeit ICs are *1) remarked/recycled*, 2) *cloned/copied design*. The former includes the selling of aged chips as new, after possibly repackaging/remarking of the die. The latter category includes unauthorized production/selling of an IC without legal rights. It is typically performed through Intellectual Property (IP) piracy at different levels, IC reverse engineering or overproduction at foundry, as shown in Fig. 1(b). Often, low-grade ICs (classified by

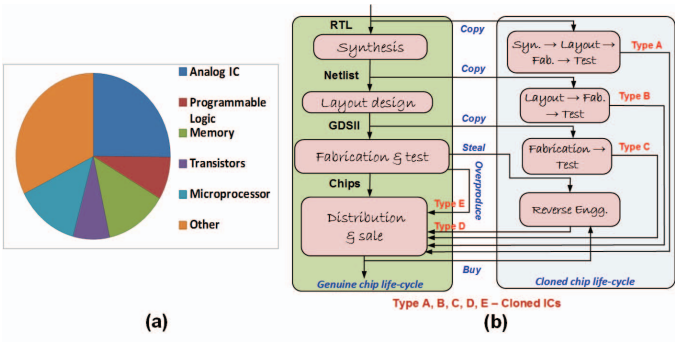


Fig. 1. a) Percentage of reported counterfeit ICs by type in 2011 [3]; (b) sneak channels used by adversaries to insert cloned ICs in supply chain.

designer after test) being sold at a higher grade by malicious entities for economic benefits is also identified as a form of cloning. The standard IC and system level tests are mostly inadequate in detecting counterfeit ICs. Furthermore, existing design-for-security (DfS) approaches are often not attractive due to significant design effort, test workload, hardware overhead and/or lack of robustness for counterfeit detection. Most of these are digital only techniques and hence inapplicable to analog chips. Besides, due to requirement of design modifications, these techniques are not suitable for legacy designs i.e. IC designs that have reached closure or pass through for fabrication. As a result of such shortcomings, many counterfeit incidences have not even been detected in recent times. To address this growing concern, there is a critical need for robust, low-overhead protection against counterfeit ICs.

In this paper, we propose a simple, robust IC authentication approach, referred to as *PiRA*, to validate the integrity of ICs in presence of cloning attacks. It exploits the intrinsic, uncontrolled, random variations in the pin resistances (PiR) within and across different ICs to create unique chip signatures for authentication (A), as illustrated in Fig. 2. Pin resistance is usually defined as the electrical resistance calculated while looking into the corresponding pin under operating conditions, similar to the concept utilized to measure input resistance/impedance at circuit nodes. It is calculated by measuring the input current for particular external DC voltage input at the pins (within specifications) in a powered chip. Powering is required to set stable working states for the active electronic components in the I/O logic. In PiRA, we extend the concept of pin resistance to incorporate the current through the port protection diodes by appropriate forward biasing in the input modes as well as the drive cur-


978-1-4673-6578-9/15/$31.00 ©2015 IEEE

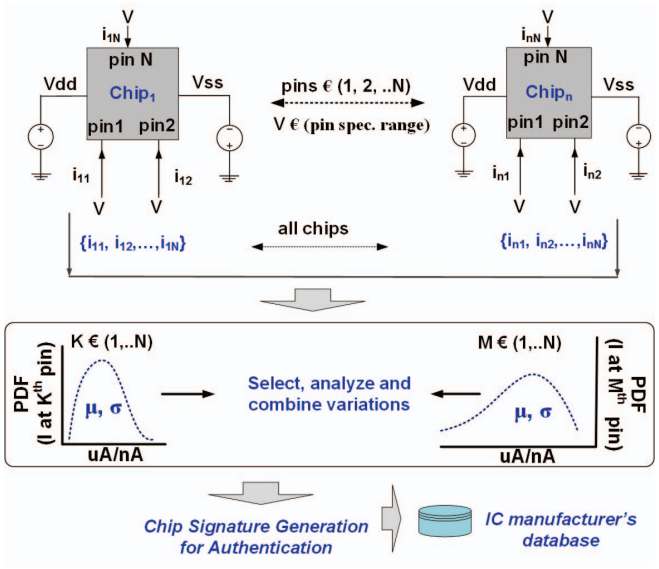


Fig. 2. Chip-specific signature creation from the intrinsic variations of pin resistances across ICs, measured by DC input/output current variations for particular voltages at pins.

rent during output mode source/sink (pin output resistance). Under normal operating input modes, the measured current is the same as the input high (IIH) and low (IIL) leakages at the logic high and low voltages, commonly measured at the digital pins to detect any defects/failures during chip testing [4], [5], [6]. It is referred to as input leakage due to extremely high input resistance at typical digital I/O ports arising mainly from i/p digital buffers/schmitt triggers as well as off-state output components. For analog chips such as operational amplifiers, the similar measurement corresponds to the small input bias currents at pins. Application of input voltages just outside the supply range (within absolute ratings) would lead to current measurements solely through forward biased diodes and likewise for load currents through source/sink driver transistors in output ON modes. We measure these different currents (inversely proportional to encountered pin resistance) and use its variations across chips to create unique signatures. During conventional IC testing, the different leakages/bias/output currents are tested simply to check if they fall within limits or meet design specifications. We propose to utilize their chip specific variations for IC authentication. Sub or super-linear resistances add to the overall signature space entropy and may be calculated from measurements at different DC current-voltage (I-V) points to generate multiple bits of signature per pin. Impedance estimation through AC measurements may lead to greater information, but this paper is limited to DC tests.

The candidate pins for authentication include all types and functions encompassing general purpose input-output (GPIO), input (i/p) as well as output (o/p) pins. Intrinsic random process variations affect the on-die I/O logic circuits. PiRA is based on extracting these variations by appropriate external current measurements. These are normalized and used for the purpose of chip authentication. The presence of high entropy per pin enables application of the approach to small scale low-pin-count ICs of all types. Besides through PiRA, one can measure variations across individual discrete components of I/O port logic, resulting in higher extracted entropy compared to most on-chip Physical Unclonable Function (PUF) based schemes, where the random variations are averaged over multiple elements to obtain the final measured parameter (e.g. delay).

PiRA only incurs some additional test effort at the end of the IC design cycle as illustrated in Fig. 3(a). The signature generation happens during this phase under the control of the IC manufacturer. The unique legitimate fingerprints are stored in the designer's secure database. The pin measurement and signature creation protocol is public. On receiving an IC from the supply chain, a system designer/integrator would generate its signature after appropriate measurements. If the signature matches any of the current entries in the database, then it is confirmed as a legitimate chip (Fig. 3(b)). A secure, verification device (VD), although not a necessity for PiRA implementation, can be passed from the designer to the system integrator for IC authentication. This provides the advantage of standardized measurements and avoids effect of site-to-site variations on signature generation. Besides, a VD performing automated authentication may lead to easier adoption of PiRA by minimizing time-to-market.

The pin resistance variations within and across chips due to process noise are uncontrolled and virtually impossible to clone for each pin of an IC. Hence, for sufficient extracted entropy and thereby large enough signature length (e.g. $\geq$ 80 bits), all chips including cloned ICs would practically possess a unique signature (different from legitimate ICs). As chips cloned through IP piracy, IC reverse-engineering and overproduction typically follow alternate routes into the supply chain, their fingerprints are not stored in the IC manufacturer's database. Hence, they would be easily detected by a trusted party e.g. system designer. Moreover, if the IC designer maintains separate databases for different grades of a chip family, a low-grade IC being sold as higher grades would be detected as well using PiRA. The chip signatures are generated at the end of the design cycle. Hence, PiRA is resistant to any information leakage and tamper based attacks. As compared to existing design-for-security techniques, PiRA provides two major advantages: **1)** It incurs virtually zero design effort and hardware overhead

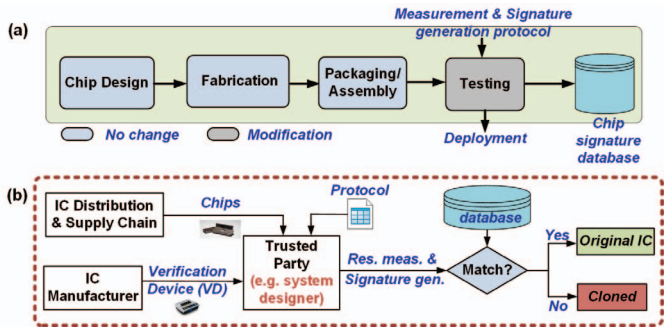


Fig. 3. a) Incorporation of the signature generation step in the IC design cycle; (b) seamless integration of PiRA with the current semiconductor business model for enhanced security.

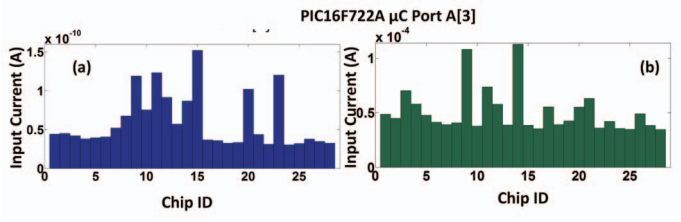


Fig. 4. Measured variation of pin input current in (a) normal operational mode (logic high i/p voltage of 5.5 V) and (b) forward-biased ESD diode (6 V i/p for $V_{dd}$ = 5.5 V) in 28 PIC micro-controller chips.

at similar protection levels as other approaches; **2)** It can be applied to legacy designs, which comprise a major portion of the market. Its usage extends to chips of all types including analog/mixed-signal ICs, in which existing all-digital security primitives are difficult to implement. In particular, the paper makes the following major contributions:

- It proposes a novel robust chip authentication approach, *PiRA* that can effectively protect against cloning based attacks. PiRA is based on unique chip signatures generated from the intrinsic, random variations in the pin resistances within and across different ICs.
- PiRA incurs virtually zero additional design effort and hardware overhead. It only requires minimal extra signature generation steps during final IC testing. It can be applied to legacy designs and is suitable for security of all chip types including analog/mixed-signal ICs.
- The paper analyses the methodology and implementation of the approach including sources of entropy, measurement scheme and the signature generation protocol. It presents comprehensive security analysis of PiRA. Moreover, experimental measurements with common ICs demonstrate the efficiency of the approach.

The remainder of the paper is organized as follows. Section II describes related work with a focus on Design-for-Security (DfS) techniques against cloning attacks. Section III presents the PiRA methodology and implementation details including signature generation scheme. Section IV analyzes the security of PiRA as well as experimental results with representative chips of different types. Finally, Section V concludes the paper and provides future directions.

## II. Related Work

Due to the inadequacy of industry level, reactive countermeasures based on standard physical, functional and reliability test/validation [1], [2], proactive approaches based on appropriate design modifications for security have emerged more attractive. For protection against cloning, they include chip tracking and authentication schemes based on watermarking [7], IC fingerprinting as well as obfuscation [8]. However, these approaches incur design modifications (often significant) with associated hardware overhead and hence, difficult to implement for mass production of ICs. There have been attempts to tag each chip with unique ID e.g. a RFID tag, but present reverse-engineering tools have become very advanced, allowing an attacker to read them [2]. Physical Unclonable Functions (PUFs) [9] exploit intrinsic random variations in the manufacturing process to generate unique identifier for each chip. However, most PUFs also incur considerable design effort, overhead, test workload for the manufacturer and cannot be applied to legacy design ICs. As most analog/mixed-signal ICs are usually fabricated at older process nodes, they are usually not suitable for PUF implementations. Hardware metering [10] 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 additional design effort and die area overhead. The paper in [11] proposes an active defense scheme against both recycling and cloning, based on one-time-programmable (OTP) antifuses in I/O logic. For protection against cloning, apart from additional design effort in [11], the OTP key, programmed by the designer is IC family specific and is vulnerable to break one-break all type reverse-engineering attacks. The proposed approach PiRA is based on intrinsic uncontrolled variations in chip I/O components and provides much higher security against cloning attacks. Besides, it incurs virtually zero design effort, overhead, lower test workload and can be incorporated in legacy design ICs and analog chips.

## III. Methodology

PiRA is based on entropy extraction from inherent, random variations in chip I/O port components to create unique signatures for authentication. The variations are captured through external pin resistance (current) measurements under different modes and varying bias conditions. The variations in the measured input pin current at logic high voltage as well as through the corresponding $V_{dd}$ forward biased protection diode (at i/p of 0.5 V greater than $V_{dd}$) of a PIC microcontroller port [12] are illustrated in Fig. 4. Before going into details of the methodology, we describe the specific threat model that PiRA targets to protect against.

### A. PiRA Threat Model

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 in a system, an IC is often bought and resold many times,

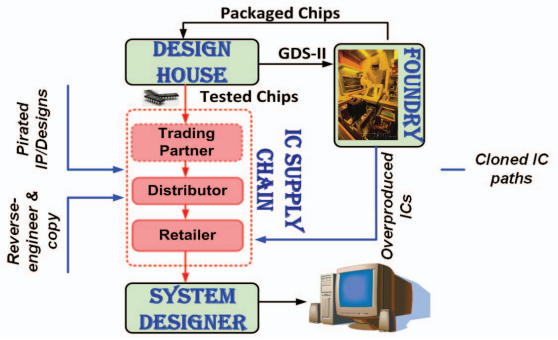


Fig. 5. The globally distributed, uncontrolled supply chain between IC manufacturer and a trusted party like system designer.

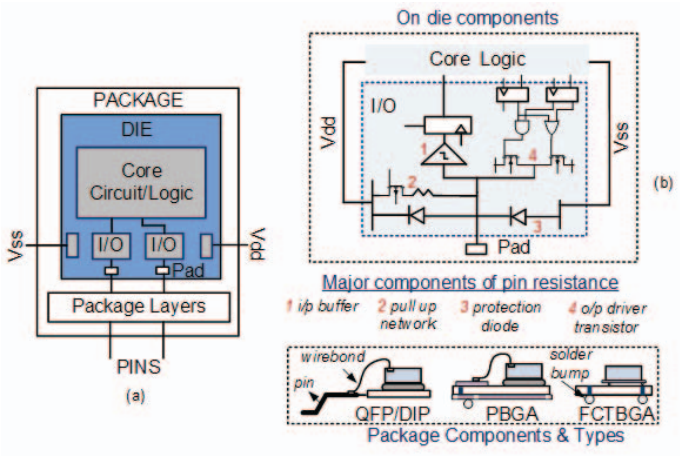


Fig. 6. (a) Schematic of typical path from IC pin to die core logic; (b) Representative on die I/O logic as well as package level components.

involving untrustworthy entities [3], [2] in a supply chain as illustrated in Fig. 5. In this paper, we consider defense against a particular major form of counterfeiting attack i.e. cloned chips. In the current business model, a trusted party such as system designer would want to make sure of the origin or authenticity of the chips he/she buys to integrate into a system. In the absence of convenient existing solutions, PiRA is proposed to detect and extract out the cloning based malpractices in the supply chain, thereby giving these trusted parties a defense platform as well as maintaining the economic benefits of the original IC designer. PiRA considers authentication of the chips till the system designer level as these cover most of the usual cloning attack pathways. As such, we do not require to analyze robustness of the signatures with aging due to normal in-field operations.

### B. Sources of Entropy

A general schematic of the electrical path from the external digital IC pins to the core circuitry through the packaging layers, contact pad and Input/Output (I/O) logic is illustrated in Fig. 6(a). A detailed diagram of representative I/O logic components on die as well as assembly/package constituents along the pin electrical path are shown in Fig. 6(b). Package level components including wire bonds, solder balls, die pads, vias etc. contribute minimally towards pin resistances. In the I/O port logic in most representative digital IC families, the input buffer (often a schmitt trigger), output pull up/down driver transistors, protection diodes to both supplies as well as optional pull up/down resistor networks (implemented usually with transistors) are the major contributors to measured pin resistances (current) under different bias conditions, applied voltage, register settings etc. For analog ICs, this could include both bipolar or CMOS transistors and different bias resistor networks.

Process variations during IC fabrication would cause intrinsic, random differences in these I/O components within and across chips, specifically the geometry, dopant concentration of the constituent transistors etc.. These lead to varying electrical properties and hence resistances of the discrete I/O components (remains within design specifications), which are captured by appropriate DC current measurements in PiRA. Independent random variations across different I/O components lead to higher entropy of signature space. Besides, through PiRA, one can measure the intrinsic variations in individual discrete components like a diode, PMOS/NMOS driver transistor etc. which preserves the underlying entropy as compared to current or delay based PUFs which perform averaging over different components.

### C. Measurement Scheme

For PiRA pin resistance measurements during normal input operations, an external voltage in the allowable range is applied at the pin and the input leakage/bias current measured with a high resolution ammeter whose range extends to $\mu$A/nA [13]. For general purpose input-output (GPIO) pins, the output path is placed in the high impedance (Z) mode before the measurement through for example writing the corresponding value in the data direction register. Lower the measured current, higher the pin resistance and vice versa. For the common digital ICs (e.g. micro-controller, FPGA, processors etc.), input voltages in the logic high (LH) and low (LL) ranges lead to activation of different pull down and pull up networks in the input path logic. In CMOS technology, PMOS based pull up and NMOS based pull down have different nominal doping types, concentrations, geometries etc. and hence the variations in the resistance for LH and LL are mostly independent (uncorrelated) of each other. This increases the signature space entropy. This can also be verified by the fact that both input high (IIH) and low (IIL) leakage tests are performed in all pins as part of IC parametric/defect tests. Empirical tests show that in digital ICs, intermediate input voltages (between LH and LL) lead to floating values and hence varying currents for different trials. Hence only two i/p voltages at the logic high and low ranges are considered for pin leakage tests in digital ICs. Multiple candidate pins can be selected from the same port as the process variations affecting each I/O path within the chip are mostly random. As different pins of a port (e.g. 8 bits of I/O port etc.) do not effect each other in terms of I/O operations, other pins may be left unconnected while measuring a particular pin. If o/p resistance and hence drive current variations are included for signature creation, the

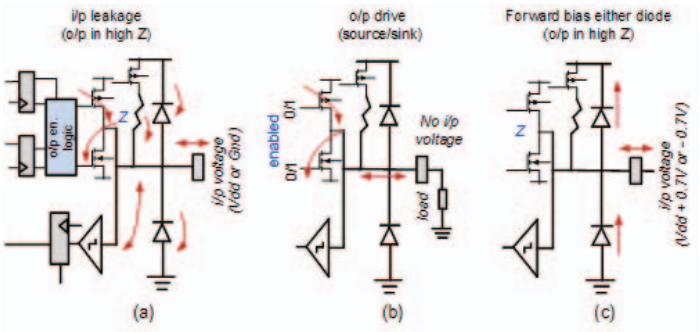


Fig. 7. (a) Typical measurement scheme of input leakage currents; extended schemes measuring (b) output drive; (c) forward-biased diode current.

corresponding pins are placed in the o/p mode. The o/p current is measured for a particular written (through internal register) high/low port voltage and fixed load across different chips. In this way, the pull up/pull down driver transistor variations may be extracted. To further incorporate protection diode variations, i/p voltages greater or less than $V_{dd}$ and $V_{ss}$ by 0.3-0.7 V (less than absolute ratings) would be applied to forward-bias either diode in the input mode and the resulting current measured. The different measurement schemes for digital I, I/O, or O pins are in Fig. 7

The measured leakage currents at both logic low and high input voltages for three pins are illustrated in Fig. 8 for three PIC micro-controller ICs [12]. Out of three pins, two are from the same port (pins 3 and 7 of port A). The measurements are performed with the high precision semiconductor analyzer instrument [13]. According to specifications, the power pins are connected to 5.5 V and 0 V respectively. The negative values for the 0 V i/p signify the reverse direction of current as compared to 5V i/p (source/sink). On careful observation, it is seen that for the 1st chip, at 0 V, the current for pin 3 of port A is slightly higher than that of the pin 7. However, the reverse is observed at the 5.5 V input. Similar is the trend (reversed comparative values at low/high i/p) for chip 2. On the contrary, for chip 3, pin 3 of port A has higher current values for both inputs as compared to pin 7, but the magnitude by which the current is higher at 5.5 V (compared to nominal) is much greater than that at 0 V. Similar analysis may be performed with the port B pin. The general comparative trend as well as the percentage deviation from inter-die nominal value are important in the final signature entropy. Hence, the variations considering same/different port pins and logic low/high input voltages add to the net chip entropy for authentication. For pure analog circuits such as op-amps, depending on existing linearity/correlation between pins (e.g. often if inverting i/p shows higher than nominal bias current, then so does the non-inv. i/p), intermediate multiple i/p voltage points, between maximum and minimum recommended values may be analyzed for inclusion into the signature space.

### *D. Signature Generation*

The signature generation scheme is chosen to utilize the extracted entropy and achieve high uniqueness and robustness of the legitimate chip signatures. For enhanced robustness, comparison of inter-pin (pins of same chip) normalized variations is preferred over other schemes such as digitization of individual pin values over the entire range. This is analogous to the comparisons between ring oscillator frequencies in RO-PUF implementations [9]. Small changes in pin currents across different iterations due to common mode (temperature/input voltage change) or other sources generally do not affect the signature bits in the said scheme. However, as compared to delay based PUFs, where all the delay paths are designed for the same nominal frequency, the individual pins (even from same port) usually have different nominal resistances, especially for input leakage current measurements. This is because pins may be multiplexed with different functions to save pin count in chips like micro-controllers, FPGAs etc. Moreover, I/O logics are designed to meet the specification limits rather than having the same nominal electrical values. As a result, to compare between pin values of an IC to generate signature, a normalization scheme has to be chosen. The scheme should distribute the pin variations around the chosen nominal parameters in an un-biased manner. Another advantage of the comparison based scheme is the rapid growth (quadratic-linear from $NC_2$, N is no. of pins) of signature space with number of candidate pins, especially beneficial in small scale ICs. This allows one to create large signatures with greater uniqueness as well as bit selection for enhanced robustness.

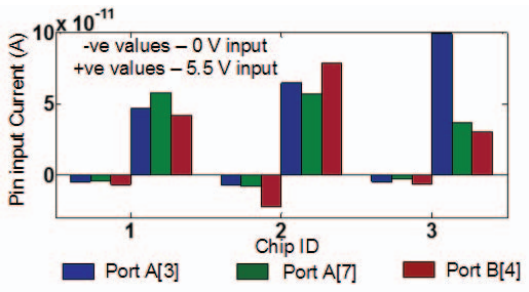


Fig. 8. Measured pin leakage currents at logic low and high input voltages for 3 different pins across 3 chips [12].

After empirical analysis, normalization of individual pin values around the corresponding global pin mean ($\mu$) and standard deviation ($\sigma$) is chosen. Here, global values refer to the $\mu$ and $\sigma$ of the measured current distribution of corresponding pin across all the chips. The IC lot, used to calculate the global values, would ideally represent the spectrum of possible variations for the chip pins. The $\mu$ and $\sigma$ of the distribution after normalization is 0 and 1 respectively. Due to such normalization, intrinsic variations in pin i/p leakages, o/p drive currents and forward biased diode currents etc. from different pins can all be incorporated into the total IC signature space, leading to utilization of the high available entropy. For example, in a digital IC where only two input voltages are selected per pin and 10 candidate pins are considered, there are 20 normalized values for each IC. For some chips, not all pins (e.g. reset, offset etc) would exhibit un-correlated variation characteristics for 2 voltage inputs. In these cases, one voltage point may be considered for a particular pin where as multiple i/p voltages for non-linear analog inputs. Two values from the entire normalized set are chosen and compared between each other to produce a 1/0 signature bit. Hence, the general formula for the total number of possible signature bits L is

$$L = SC_2,$$

S is the total possible comparisons. Often in digital ICs,

$$S = (M * N)C_2,$$

M is average number of independent readings per pin and N is the number of pins.

The maximum number of parameters per digital I/O pin is usually 6 (2 i/p, 2 o/p, 2 diode currents). Hence even just 3-4 such pins could provide a large signature data set. For purely analog I/O, amount of data per pin vary with different chip

types. The large signature space allows for non-robust, biased bit removal and maintain a unique signature greater than for example $\sim 80$ bits. It is empirically observed that non-robust bits are caused due to comparison between two close (almost equal) normalized values. Hence, across the sample set of chips, non-robust and/or biased comparisons are removed by automated methods. Through testing it is often seen that particular individual pin/s cause non-robust signature bits and should be discarded from analysis. The chosen normalization parameters, comparison pairs and the particular order for signature creation are applied to all manufactured ICs. To account for possible widely varying IC pin leakage currents due to different foundries etc, the normalization parameters may be updated following different protocols, but is not analyzed here. The IC signature generation steps are enumerated-

---

**Signature Generation Steps**

**Input**:

$[I_j]$, the parameter vector of chip,
$[M_j]$ & $[SD_j]$, mean, standard dev. for each j,
$C \subseteq S$, C$\leftarrow$ select comparison pairs for IC
for $j \subseteq (1, .., N)$, N$\leftarrow$no. of parameters (pins, voltages)

**Normalization**:

for all $i \subseteq (1, .., N)$,
$T_i = (I_i - M_i)/SD_i$
end

**Comparison**:

co $\leftarrow$ 0
for all $i \subseteq (S)$,
for all $j \subseteq (S)$, j $\neq$ i, $(i, j) \subseteq (C)$
co $\leftarrow$ co + 1
If $T_i >= T_j$
$P_s[co]$ = 1
else
$P_s[co]$ = 0
end
end

**Output**: Sig = $[P_s(k)]$, $k \subseteq (1, .., L)$, L$\leftarrow$ $|C|$

---

## IV. Security Analysis

In this section, we analyze the security of the proposed approach from the aspect of probability of copy of any legitimate signature by malicious adversaries. Besides, through experimental measurements, two commonly used chips are verified for high uniqueness and robustness of signatures.

### A. PiRA Security

With PiRA, along with cloning the design, an adversary needs to copy a legitimate chip signature to pass authentication. For most chips, PiRA implementation reduces probability of cloning signatures to virtually zero.

**1)** PiRA is based on intrinsic, uncontrollable variations in pin resistances within and across chips. The variations are mainly due to intra and inter-die random process variations in the I/O logic. The entropy of signature space is increased by choosing variations across multiple individual I/O components at different independent voltages per pin. 8-10 candidate pins with just logic high and low i/p voltages can easily allow a minimum of 80 bit IC signature. The resistance looking into IC pins follows different distributions (different $\mu$ and $\sigma$) for different pins. IC design is performed to only constrain them within specified limits rather than achieve same nominal values etc. Hence, the varying distributions renders it virtually impossible for attackers to replicate them for each pin of an IC. The inherent randomness of sampled values due to manufacturing processes would lead to unique combination of leakage currents for all ICs, including malicious chips. With a maximum of 1-10 million chips ($\sim 2^{23}$) of a kind produced, a $>$ 70-80 bit signature renders all attempts by an attacker futile in copying any legitimate IC signature while maintaining any economic benefits.

**2)** In case of small size of signature space (e.g. 6 pins in a voltage regulator IC), the comparison based signature generation may suffer from a security weakness in the fact that an attacker does not require to copy the individual legitimate pin resistance distribution for cloning. As normalization removes all effects of nominal values in parameters, an attacker can copy an IC signature even by entirely different distributions. ICs with enough randomly varying candidate parameters would automatically reject any such attacker attempts. PiRA can incorporate an additional step in signature verification to overcome any such weaknesses for very small scale chips. During authentication, the pin currents would be measured and during normalization would be compared with IC designer chosen nominal values. If any value/s lie outside legitimate distributions, then the IC is rejected even if signatures match. This additional step further strengthens the defence of PiRA for small chips with limited number of authentication parameters.

### B. Uniqueness and Robustness of Signature

We experimentally measured pin currents and generated signatures for 28 PIC 16F722A micro-controller ($\mu$C) chips [12] and 22 LM741 op-amp ICs [14]. Although a larger sample set for both would have led to a better representation

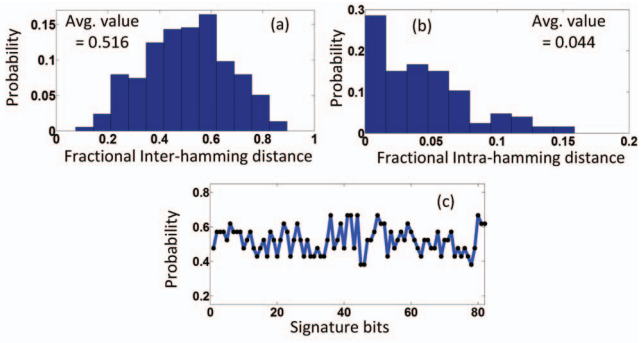


Fig. 9. (a) Fractional Inter-Hamming and (b) Fractional Intra-Hamming distance (5 repetitions) for 82 bit signatures across 28 PIC $\mu$C ICs; (c) Probability of 1 of signature bits.

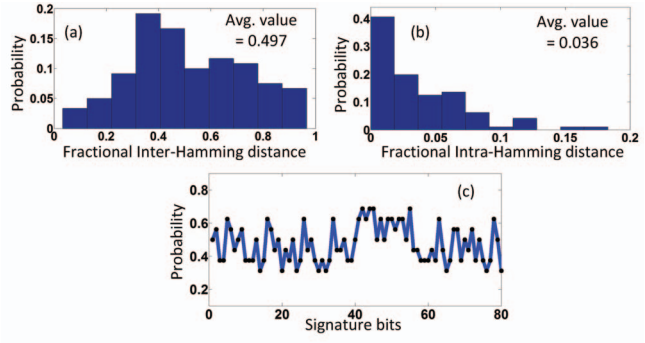


Fig. 10. (a) Fractional Inter-Hamming and (b) Fractional Intra-Hamming distance (5 repetitions) for 80 bit signatures across 22 OP-AMP ICs; (c) Probability of 1 of signature bits.

of the signature space, the empirical measurements serve only to verify the feasibility and efficiency of the proposed approach. For the 28 pin $\mu$C chips, 8 pins were considered with two voltage (logic high of 5.5 V and low of 0V) inputs per pin. There are more candidate pins, but 16 ($8X2$) considerably independent IC pin parameters lead to 120 ($16C_2$) possible signature bits. The 8 pins include 3 pins of port A (IC pin 1, 3 and 5), 3 pins of port B (IC pin 14,15 and 16) and 2 pins of port C (IC pin 24, 28). All $\mu$C pins are multiplexed with other functionalities (e.g. clock, ADC input, reset) and hence have different distributions. With $V_{dd}$ and $V_{ss}$ of 5.5 V and 0 V, the leakage currents are measured in normal input mode. A high end, state of the art characterization system with sub-pA current resolution [13] is used for measurement. In a suitably controlled environment (ambient temperature of $25°C$ and minimal disturbances), each chip is placed on the socket and readings conducted. Same socket and probe wires, cables are used for all chips to avoid any effect of external variations. Each measurement is repeated 8 times around the same instant and the average taken to remove random measurement noises. The measurements for each chip are also repeated on 5 different days with $\sim 5-10°C$ ambient temperature differences to test for robustness at different temporal instants. We had used the same measuring instrument. A verification device (VD), exchanged between IC manufacturer and system designer (as mentioned earlier) can be used for these standardized measurements across different sites. The metric for signature uniqueness [9] is the fractional Inter-Hamming distance and its average is:

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

$HD_{ij}$ is the fractional Inter-Hamming distance between chips i and j and N is the number of chips. $HD_{inter}$ is desired to be $\sim 0.5$. Signature robustness has been quantified by the fractional Intra-Hamming distance distribution [9] with average value ($HD_{intra}$) as:

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

Here $HDI_{ijk}$ is the fractional Intra-Hamming distance for chip i between the $j^{th}$ and $k^{th}$ measurements. Here Z = 5. $HD_{intra}$ should be ideally around zero. Besides, a third quantity providing an estimate of the randomness of individual signature bits (hence presence of any bias) is given by the probability of 1/0 of the bits over all ICs.

After normalization, it was observed that parameter values varied by a maximum of 2-2.5 $\sigma$ around mean. For the PIC 16F722A, considering all 120 signature bits, the robustness was an issue, with the average $HD_{intra}$ being equal to $\sim 9\%$. The Inter-Hamming distribution was centered around an average of $\sim 0.5$, but the distribution was very wide. A few bits were biased to 1 or 0 (probability greater than 0.75 across chips). After thorough post-measurement analysis, the above-mentioned degradations could not be only attributed to a particular pin or set of pins. Rather, different comparisons between normalized values contributed towards them. These non-robust and/or biased ones are removed by setting appropriate thresholds. The outliers in the inter-hamming distributions were analyzed for reduction as well. The final fractional Inter-Hamming distance distribution for the selected 82 bit signature is illustrated in Fig. 9(a), with an average of 0.516. The same for the Intra-Hamming distribution is shown in Fig. 9(b), with an acceptable average of 0.044. Fig. 9(c) shows that none of the bits are biased with probabilities of 1 being between 0.4 to 0.63.

For the op-amp LM741, measurements were conducted with positive and negative supply voltages of 15 and $-15$ V. Only 5 pins are candidate pins for PiRA in the 8 pin IC. These are the two inputs, two offsets and the output pin. Although the supply values allow for wide input voltage range at the pins, only 4 voltage points for the 2 i/p pins are considered due to significant linearity (correlation) in pin currents at multiple voltage points for a pin. Similarly, only 2 measurement voltages are considered for the two offset pins and 3 for the output pin. These points were considered from the analysis of increasing percentage of non-correlated variation around the nominal (different linear slopes for different ICs) across chips. Inclusion of more voltage inputs does not really increase the net entropy. Additionally, a 1 K $\Omega$ resistor is connected in series with both offset pins for all

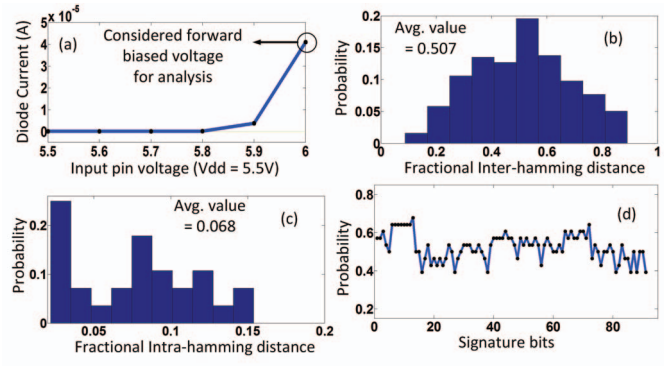


Fig. 11. (a) Forward-biased diode voltage selection; (b) Fractional Inter-Hamming and (c) Fractional Intra-Hamming distance (5 repetitions) for 91 bit signatures considering both $V_{dd}$ and $V_{ss}$ diodes in 7 I/O ports across 28 PIC $\mu$C ICs; (d) Probability of 1 of each signature bit.

chips to reduce the high current range to measurable values. Overall 15 nominal parameters were calculated per IC, with total of 105 signature bits. After similar analysis as the $\mu$C, bits were removed for increased uniqueness/robustness. The corresponding op-amp metrics (Fig. 10(a),(b) and (c)) for 80 bit signature are within acceptable limits for authentication.

Apart from normal mode pin resistance measurements, signatures of the 28 $\mu$C chips have also been created from forward biased protection diodes at the pin inputs. Both $V_{dd}$ and $V_{ss}$ diodes have been considered for analysis in 7 pins, namely 3 of port A and 2 each for ports B and C. More no. of pins can be easily considered to extract higher entropy. The forward biased diode resistance has been measured at an i/p voltage which is 0.5 V outside the supply ranges (Fig. 11(a)), still within the absolute ratings. The currents are in the range of 50 $\mu$A. For these 14 normalized parameters (2 diodes per IC pin) for every chip, 91 bit signatures have been created without any particular biased or non-robust comparisons. As in the previous scenario, measurements were repeated on 5 separate days for robustness analysis. The metrics for overall signature quality, considering only IC port diodes is illustrated in Fig. 11(b), (c) and (d) and are well suited for IC authentication. Removal of 4-5 comparisons can bring $HD_{intra}$ down to 4.2%. Although not performed here, load current measurements for driver source/sink transistors can be done similarly for a fixed load resistor in the port output modes to extract further entropy. Hence efficiency of PiRA has been verified experimentally for sample ICs.

### C. Discussion

Apart from the micro-controller and the op-amp, we analyzed the feasibility of PiRA in a discrete SRAM memory chip as well [15]. Due to constraints of time, we had analyzed the signatures in 25 SRAM ICs with leakage measurements in 10 input pins, namely 8 address pins and 2 control pins (output enable and chip enable) at logic high and low voltages. 135 bit signatures were generated for each IC after removal of some biased bits and analyzed for uniqueness. The results are shown in Fig. 12(a) and (b). Multiple iterations of SRAM measurements would be done to test for robustness in the future. The calculated uniqueness metric values are a major step towards verifying implementation of PiRA in SRAM memory chips.

A better controlled automated precise measurement setting, available in industries would lead to better quality of signatures. Moreover, the ICs considered in the paper are manufactured at much older process nodes. The efficiency of PiRA would increase for higher process variations in ICs fabricated at recent technologies. For PiRA, authentication is till the system designer level, which is sufficient for protection against most cloning attacks. Research would be conducted to analyze signature robustness with aging and hence potential for in-field authentication.

## V. Conclusion

We have presented a simple, novel IC authentication scheme, *PiRA*, to protect the integrity of chips against all

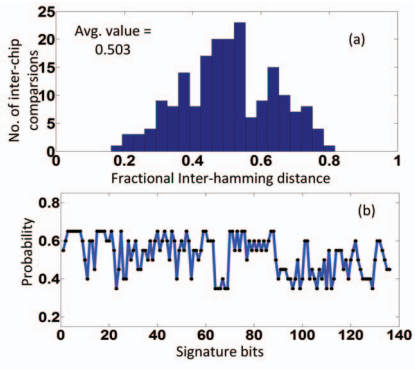


Fig. 12. (a) Fractional Inter-Hamming distance for 135 bit signatures in 25 SRAM ICs (good uniqueness); (b) Probability of 1 of each signature bit.

forms of cloning attacks. PiRA exploits the random intrinsic variations of pin resistances within and across ICs to create chip-specific signatures for authentication. For example, pin resistances in the normal input mode can be obtained by measuring the input leakage/bias currents at pins, analogous to the input high and low leakage based defect tests in ICs. Signatures are generated in PiRA by incorporating multiple I/O logic components per pin to increase the overall entropy. Compared to existing design-for-security techniques, PiRA has a major advantage of incurring virtually zero design effort and hardware overhead. Furthermore, it can be applied to ICs of all types including analog/mixed signal ICs. PiRA is suitable for legacy design chips as well.

The paper discusses the possible sources of variation of pin resistance, the measurement scheme for PiRA as well as the signature generation for authentication. Security has been analyzed against all possible cloning attack modes. Finally, experimental measurements for sets of commonly used digital and analog IC prove the effectiveness of the scheme. Future research would include extension of PiRA to in-field authentication and to different chip types.

## 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] "Counterfeit Chips on the Rise", *http://spectrum.ieee.org/computing/*.
[4] "Leakage Curve Test", *http://www.semitracks.com/*.
[5] "DC Characterization of ICs Using PXI Instrumentation", *http://www.marvintest.com/*.
[6] "Apparatus for testing input pin leakage current of a device under test", *US Patent 4862070 A*.
[7] A. B. Kahng et. al, "Robust IP Watermarking Methodologies for Physical Design", *DAC*, 1998.
[8] R. Chakraborty et. al, "RTL Hardware IP Protection Using Key-Based Control and Data Flow Obfuscation", *VLSI Design*, 2010.
[9] S. Devadas et. al, "Physical unclonable functions for device authentication and secret key generation", *DAC*, 2007.
[10] F. Koushanfar et. al, "Active Hardware Metering for Intellectual Property Protection and Security", *USENIX Security*, 2007.
[11] A. Basak et. al, "Active Defense against Counterfeiting Attacks through Robust Antifuse-based On-Chip Locks", *VTS*, 2014.
[12] "PIC16(L)F722A/723A Data Sheet", *http://www.microchip.com/*.
[13] "Model 4200-SCS Semiconductor Characterization System", *http://www.keithley.com/*.
[14] "LM741 Operational Amplifier", *http://www.ti.com/*.
[15] "32K *X* 8 LOW POWER CMOS STATIC SRAM", *http://www.issi.com/*.