2020 IEEE International Test Conference (ITC) | 978-1-7281-9113-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/ITC44778.2020.9325209

Schmitt Trigger-Based Key Provisioning for Locking Analog/RF Integrated Circuits

A. Sanabria-Borbón*, N. G. Jayasankaran*, S. Lee*, E. Sánchez-Sinencio*, J. Hu*†, and J. Rajendran*
*Department of Electrical and Computer Engineering, †Department of Computer Science and Engineering
Texas A&M University, College Station, Texas, USA
Email: {adca.sanabria, gjn, lov4holic, s-sanchez, jianghu, jv.rajendran}@tamu.edu

***Abstract*—Analog/RF performance locking techniques insert configurable components to obfuscate the biasing or the design parameters of the secured analog block. The locked circuit meets the specifications only under a specific configuration decided by the correct common key, shared by all chip instances of the same design. Key provisioning enables the design of distinct user keys for individual chip instances. This area has received little research attention, and a naive approach yields large area overhead when increasing the key size. We propose a new approach based on a Schmitt trigger (ST) circuit with configurable hysteresis. The proposed key provisioning is compatible with existing analog locking techniques and has a constant area overhead regardless of key size. This approach is tested with three analog/RF circuits to demonstrate its area scalability and effectiveness on security.**

I. Introduction

A. Motivation

The increased cost in fabricating integrated circuits (ICs) has led many semiconductor companies to go fabless. These companies face challenging security threats due to the outsourcing of IC fabrication. Security threats include intellectual property (IP) piracy, overproduction, reverse engineering, counterfeiting, and hardware Trojans [1]. Several design-for-trust (DfTr) techniques such as logic locking, camouflaging, and split manufacturing are proposed to secure digital circuits [2–5] and analog circuits [6–12] against these threats. Logic locking is the most preferred DfTr technique as it protects the circuit from an untrusted foundry and an untrusted end-user, whereas other techniques protect the circuit from only one of them.

In digital logic locking [2, 5], the circuit is encrypted by inserting key-gates, additional gates connected to the key inputs. When the correct key is applied, the design functions as intended. Otherwise, applying an incorrect key produces an incorrect output.

Similarly, in analog locking [7, 9, 13], the key inputs control design parameters like the biasing (voltage or current) or the effective sizes of the transistors (channel length L and width W). Since these parameters have a direct impact on the circuit's response, its performance metrics are locked. Only the correct key configures these parameters such that the circuit performs as per specifications. Otherwise, the error between the measured circuit's response and the specified one is larger than the acceptable tolerance. All instances of the protected circuit share the same key, *a.k.a*, the common key (CK). This key is the designer's secret and is available only to the authorized user.

The CK is either stored in a tamperproof memory, as in [5], or generated by a **key provisioning** unit [2, 7]. In [5], if the attacker finds the CK, then all the instances of the same design can be unlocked using this key [14, 15]. A key provisioning technique helps in addressing this issue. As shown in Fig. 1, this block takes in the user key (UK), and generates the CK, which is equal for all the instances of the locked analog circuit. A key provisioning unit ensures that each chip instance can be unlocked only by the UK, which is unique to that instance.

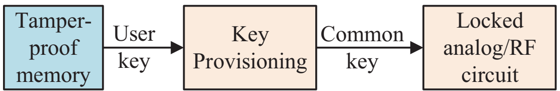


Fig. 1: The key provisioning unit generates the common key using the user key which is unique to that chip instance.

B. Related works on key provisioning techniques

Ending piracy of integrated circuits (EPIC) was the first work proposed on key provisioning [2]. It uses a physically unclonable function (PUF) or a true random number generator (TRNG), and RSA encryption to remotely activate a locked chip. The protocol for remote activation is as follows:

Step 1: As illustrated in Fig. 2, the designer locks the circuit with a CK and embeds his/her public master key (MK-Pub) in the circuit. Only the designer knows the secret CK. A PUF/TRNG and an RSA module are also inserted in the chip. The locked design is sent to the untrusted foundry, where the chip is manufactured and tested. The testing process does not require to load the key into the chip [16].

Step 2: On the first power-up, the manufactured chip generates the public and the private random chip keys RCK-Pub and RCK-Pri, respectively, using the PUF/TRNG. The foundry sends the RCK-Pub to the designer.

Step 3: The designer encrypts the CK with RCK-Pub. This can be decrypted only with the RCK-Pri generated inside the locked chip by a PUF/TRNG. For authentication, the encrypted CK is signed using the MK-Pri to generate the UK.

Step 4: The UK is sent to the foundry to activate the locked chip. The RSA module inside the locked chip authenticates the UK with MK-Pub and then decrypts it using RCK-Pri to obtain CK, thereby activating the locked chip.

Fig. 3 shows another key provisioning technique [7]. In this work, a PUF produces an individual chip ID for each chip instance [17]. This chip ID is XORed with the UK to provide the CK. The UK is unique for each chip instance.

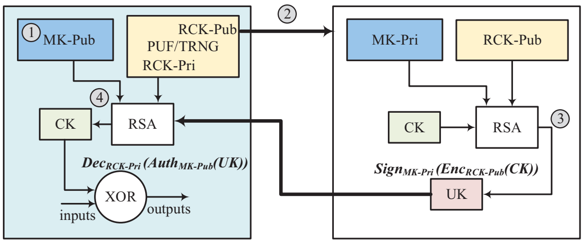

Chip at foundry
IP owner
1
MK-Pub
RCK-Pub
PUF/TRNG
RCK-Pri
2
MK-Pri
RCK-Pub
4
CK
RSA
CK
RSA
3
$Dec_{RCK\text{-}Pri}(Auth_{MK\text{-}Pub}(UK))$
$Sign_{MK\text{-}Pri}(Enc_{RCK\text{-}Pub}(CK))$
XOR
inputs
outputs
UK

Fig. 2: EPIC protocol for remote activation of the locked chip using public key cryptography [2]. Master key (MK), random chip key (RCK), common key (CK), user key (UK), public (Pub), private (Pri).

978-1-7281-9113-3/20/$31.00 ©2020 IEEE

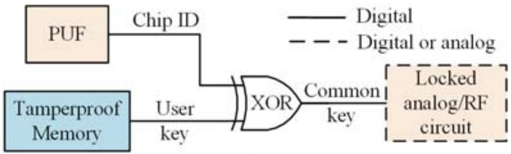


Fig. 3: In the combinational lock [7] the key provisioning generates the common key from the unique user key with the aid of a PUF [17].

In general, a key provisioning technique should have the following properties:

1) each chip instance should have a unique UK,
2) given the UK, the attacker should not be able to recover the CK, i.e., the output of the provisioning unit should be unintelligible to the attacker, given the UK, and
3) low power and area overheads.

C. Limitations of existing key provisioning techniques

The EPIC work [2], which uses a PUF and an RSA module, remotely activates the locked chip. Hence, there is no requirement for a tamperproof memory as the UK is public. However, using the RSA module for one-time CK generation cannot be justified for the area overhead it incurs [2]. Moreover, a standalone PUF has the following limitations:

- It is not suitable for generating the CKs as their output is not deterministic and stable with process, voltage, and temperature (PVT) variations [18]. There have been many attacks on the PUFs based on statistical and machine learning techniques [19, 20].
- Its size increases as the size of the chip ID required increases. For example, in [21], each six-transistor Schmitt trigger (ST), generates a one-bit response. Hence, for an n-bit chip ID, the outputs of n PUFs should be concatenated.
- It is not compatible with analog UKs.

Although many logic locking approaches have been proposed across digital and analog domains [2, 5–7], there has been very little systematic research on key provisioning techniques. Therefore, to address the limitations in existing techniques, we propose a generalized ST-based key provisioning unit with low-area overhead that is compatible with any digital or analog locking approaches, like those listed in Table I. In the proposed technique, the CK and the UK can take either digital or analog values.

D. Contributions and paper organization

We propose an ST-based key provisioning technique. This circuit takes in the UK, which is unique for each chip. It generates the CK required to unlock the analog and digital circuits locked using various logic locking techniques [6–8, 10, 11]. The contributions of this work are:

1) We propose a key provisioning technique based on the ST circuit. The conventional ST operation is enhanced with dynamic hysteresis and inversion of the thresholds to create a CK with the desired security properties.
2) The ST-based technique generates a unique UK for each chip. We use the Hamming distance as a metric of the uniqueness of the UK.
3) The UK contains most of the ST's configuration. The remaining information is stored in on-chip fuses, written before the chip's distribution. It increases the effort of reverse engineering attacks.

TABLE I: Existing digital and analog locking techniques and their user key (UK) and common key (CK) types. The proposed key provisioning technique receives the UK and generates CK. It is compatible with analog and digital keys.

Locking technique	**Digital**		**Analog**	
	UK	CK	UK	CK
EPIC [2]	✓	✓	✗	✗
Stripped functionality logic locking [5]	✓	✓	✗	✗
Combinational lock [22]	✓	✓	✗	✗
Memristor-based protection [6]	✓	✓	✗	✗
Parameter-biasing obfuscation [10]	✓	✓	✗	✗
AMS lock [23]	✓	✓	✗	✗
Mixlock [11, 24]	✓	✓	✗	✗
Analog performance locking [9]	✗	✗	✓	✓

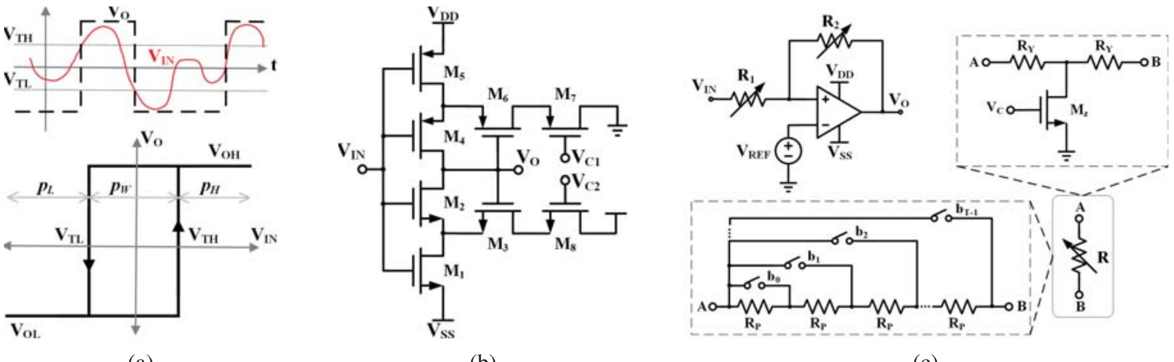
4) The proposed technique for key provisioning has a smaller area overhead compared to the existing approaches [2, 22]. In our technique, the UK is divided into segments applied serially to reuse the same circuitry. Hence, the area remains constant and independent of the key size.
5) The output, or CK, is deterministic for every input and robust to PVT variations.
6) The efficacy of this key provisioning technique is demonstrated on different locked analog circuits: a Gm-C bandpass filter (BPF), a common-gate low-noise amplifier (CG-LNA), and a low-dropout voltage regulator (LDO).
7) We present a new metric to evaluate key provisioning, namely entropy. This metric is used to estimate the effective size of the key generated by the proposed key provisioning.

The paper is organized as follows. Section II explains the working and circuit topologies of the ST.It also describes the dynamic thresholds and the window comparator required to increase the security level of the CK generated by this technique. Section III explains the proposed ST-based key provisioning technique and its security metrics. Section IV shows the experimental results of this technique, including its security metrics and its application to the locking of three circuits, namely, a BPF, a CG-LNA, and an LDO. Section V describes several analog locking approaches that can leverage the security properties of the proposed key provisioning technique. Finally, Section VI concludes the paper.

II. Background

A. Schmitt trigger (ST)

An ST is a comparator with hysteresis that uses positive feedback to amplify the difference between the input voltage (V_{IN}) and the threshold voltages (V_{TL} and V_{TH}). This difference produces an output voltage (V_O) that takes either low (V_{OL}) or high (V_{OH}) voltage values. Hysteresis refers to the dependency of the current output on the previous output [25]. Fig. 4(a) shows an example of the input and output waveforms of a non-inverting ST in the transient domain, on top, and its voltage transfer characteristic (VTC), on the bottom. The hysteresis window (HW) is the region in which the current output depends on the previous output. The width of this window is given by $HW = V_{TH} - V_{TL}$. Therefore, varying the threshold voltages varies the width of the HW. This work considers the following ST topologies: (i) internal feedback



(a) (b) (c)

Fig. 4: (a) Voltage response of a non-inverting ST (top) transient response: while the output values are either V_{OL} or V_{OH}, the input voltage takes any value in between. (bottom) Voltage transfer characteristic. (b) Internal feedback or 6-T ST. The thresholds are defined by the sizing of the transistors M_3 and M_6 and the control voltages V_{C1} and V_{C2}. (c) The external feedback ST uses an amplifier with resistors implementing positive feedback. The programmable resistors can be controlled by a digital word $\{b_0, b_1, b_2, ..., b_{T-1}\}$ or a control voltage V_C.

STs based on inverters, and (ii) external feedback STs based on operational amplifiers [25–27]. Note that although this work discusses only the non-inverting ST configuration, an inverting ST configuration can also be used.

1) Internal-feedback Schmitt Trigger (ST)

The CMOS 6T-ST circuit is based on six transistors ($M_1 - M_6$) and internal feedback, as shown in Fig. 4(b). The transistor sizes and the technology parameters define the threshold voltages of the ST. An additional transistor pair (M_7, M_8) with the corresponding control voltages (V_{C1} and V_{C2}) allows changing the width of the HW [26, 28].

2) External-feedback Schmitt Trigger (ST)

A non-inverting ST can be implemented with a high gain amplifier and external positive feedback realized by the programmable resistors R_1 and R_2, as shown in Fig. 4(c) [25]. The ST's thresholds voltages can be written as

$$V_{TL,TH} = \frac{V_{REF}(R_1 + R_2) - (R_1 \times V_{OH,OL})}{R_2} \tag{1}$$

where V_{REF} is a reference voltage applied to the inverting input terminal of the amplifier. The amplifier's output swing defines the values of V_{OL} and V_{OH} [25].

The implementation of the programmable resistors varies depending on whether the controlling input is digital or analog, as shown in Fig. 4(c). In the former case, an array of T resistors are connected via switches. These switches are controlled by the digital input $\{b_0, b_1, b_2, ..., b_{T-1}\}$, which in turn determines the equivalent resistance. Similarly, a T-network formed by R_Y and M_Z implements an analog programmable resistor, as illustrated in Fig. 4(c). The effective resistance of the T-network is a function of R_Y and the on-resistance of M_z, controlled by the voltage V_C [25].

B. Output transition probabilities of the non-inverting Schmitt trigger (ST)

The comparison of the input voltage with the threshold voltages that leads to the output being low of high defines the output transition probabilities. As shown in Fig. 4(a), p_L is the probability of $V_{IN} < V_{TL}$ thus, $V_{OUT} = V_{OL}$ and p_H is the probability of $V_{IN} > V_{TH}$ thus, $V_{OUT} = V_{OH}$. p_W is the probability of $V_{TL} < V_{IN} < V_{TH}$, where the output voltage retains the previous value. The V_{TL} and V_{TH} are configurable via the resistor settings, as illustrated in the previous section. Hence, it is possible to change the output transition probabilities by modifying the threshold voltages, i.e., the width of the HW. This work leverages the varying output transition probabilities for increasing the security of the generated CK.

C. Window comparator

Similar to the ST, in the window comparator, the output voltage is determined by the comparison of V_{IN} with V_{TL} and V_{TH}. However, as shown in Fig. 5(a), the output voltage equals V_{OH} if the input voltage lies between the thresholds, i.e., $V_{TL} < V_{IN} < V_{TL}$. Otherwise, the output voltage equals V_{OL}. As shown in Fig. 5(a), a voltage divider formed by the programmable resistors R_A, R_B, and R_C generates the required threshold voltages V_{TL} and V_{TH}. Equations (2) and (3) give the relationship between the threshold voltages and the resistors.

$$V_{TL} = (V_{OH} - V_{OL}) \times \frac{R_C}{R_A + R_B + R_C} \tag{2}$$

$$V_{TH} = (V_{OH} - V_{OL}) \times \frac{R_C + R_B}{R_A + R_B + R_C} \tag{3}$$

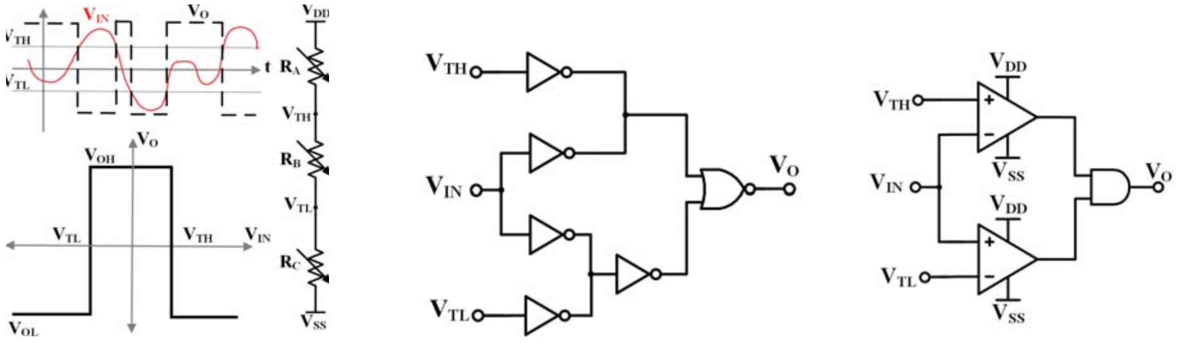
Similar to the ST circuit, we discuss two possible implementations of the window comparator. While Fig. 5(b) shows a window comparator built from logic gates, Fig. 5(c) shows an implementation based on amplifiers.

1) Inverter-based window comparator

A window comparator compatible with the internal feedback ST is shown in Fig. 5(b). This comparator is based on digital gates and has a transistor count of 14 [29]. Since the voltage divider in Fig. 5(a) sets the threshold voltages, the technology's standard gates can be used on this implementation.

2) OpAmp-based window comparator

The amplifier-based window comparator uses two high gain amplifiers as level detectors whose outputs are sent to the AND gate to produce the final output V_O, as shown in Fig. 4(c) [25]. Thus, only when the outputs of the two amplifiers are high, the output of the AND gate is high as well.



(a) (b) (c)

Fig. 5: (a) Voltage response of a window comparator (top) transient response: if $V_{TL} < V_{IN} < V_{TL}$ the output is V_{OH}, otherwise V_{OL}. (bottom) voltage transfer characteristic. The low and high thresholds are defined by the configurable resistors R_A, R_B, and R_C. (b) Inverter-based window comparator. (c) OpAmp-based window comparator.

III. Proposed approach

A. Threat model

Our threat model is identical to the one considered by analog IP protection techniques [6–8, 10]. The attacker can be in the foundry or can be an end-user. The attacker in an untrusted foundry has access to minimal resources sufficient to overproduce the chip and sell the excess chips in the black market. However, he/she cannot modify the existing layout or perform internal probing. The attacker can gain access to:

1) The layout or design masks from the untrusted foundry.
2) The process design kit (PDK) details from the foundry.
3) The netlist of the circuit extracted through reverse engineering techniques.
4) A functional chip, which has the key loaded, *a.k.a*, oracle.
5) The circuit specifications of the chip from the datasheet.

B. Schmitt trigger (ST)-based key provisioning

For a given analog input voltage and a HW configuration, the ST generates the corresponding binary output. As described in Section II-A, the output bit is a function of the input voltage, the lower and upper threshold voltages, and the previous output. When a sequence of n input voltages is applied to the ST, it delivers a series of n 1-bit outputs. These outputs are concatenated to form an n-bit output.

The proposed approach uses this operation for key provisioning. While the UK defines the thresholds and the input values, the generated digital output corresponds to the CK. The CK controls the locked circuit. To increase the attack effort, we use variable HW settings, and to achieve uniform distribution of the CK, we use positive and negative STs.

Hysteresis window (HW) settings. A fixed configuration of the HW leads to a weak defense approach. It is because the values of the thresholds can be obtained by applying increasing and decreasing input voltage sweeps and observing the corresponding output transitions. Therefore, we propose to have a dynamic hysteresis configuration. Depending on the chosen ST topology, the width of the HW can be changed by varying the input control voltages V_{C1} and V_{C2}, as illustrated in Fig. 4(b), or by tuning the resistors R_1 and R_2 for the topology shown in Fig. 4(c). Some particular settings of the HW configuration are permanently written before to ensure the uniqueness of the UK for each chip instance. Those settings are stored on-chip fuses written by the holder of the IP rights.

Positive and negative STs. The VTC of the non-inverting ST, *a.k.a*, positive ST, is illustrated in Fig. 4(a). Its transition probabilities, discussed in Section II-B, prevent the ST's output from having a uniform distribution. To compensate for that, we introduce the negative hysteresis ST. A negative ST has the values of lower and higher threshold voltages interchanged. Hence, when the input voltage is within the HW, the current output is equal to the previous output inverted. In consequence, the transition probabilities of the negative ST are complementary to the positive ST.

The output response of the negative ST is achieved by XORing the responses of the positive ST and the window comparator, configured for the same threshold voltages, as illustrated in Fig. 6. A multiplexor (MUX) selects between the response of the positive or negative ST. A one-bit sel controls the select line of this MUX. It is necessary to set the sel to 0 and 1 with equal probability to ensure that the output response has a distribution closer to a uniform one.

Fig. 7 illustrates the proposed ST-based key-provisioning. The UK and the CK can take either digital or analog values. The UK is divided into x segments that are applied in series to reuse the same circuitry. Each segment consists of three parts: (i) w bits (or analog voltage values) to configure the width of the HW, (ii) n input values consisting of a m-bit (or an analog voltage) each, and (iii) a one-bit sel (or a single voltage) that selects between the positive and the negative STs, as shown in Fig. 7.

The operation of the proposed key provisioning is as follows. In each segment, the w bits (or the analog voltage values) configure the programmable resistors that set V_{TH} and V_{TL}, defining the width of the HW. For a digital UK, a

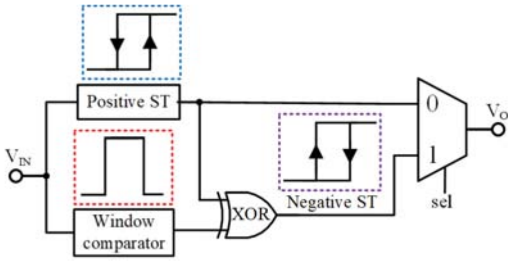


Fig. 6: A negative hysteresis ST and its voltage transfer characteristics. This is built from a conventional positive (non-inverting) ST and a window comparator.

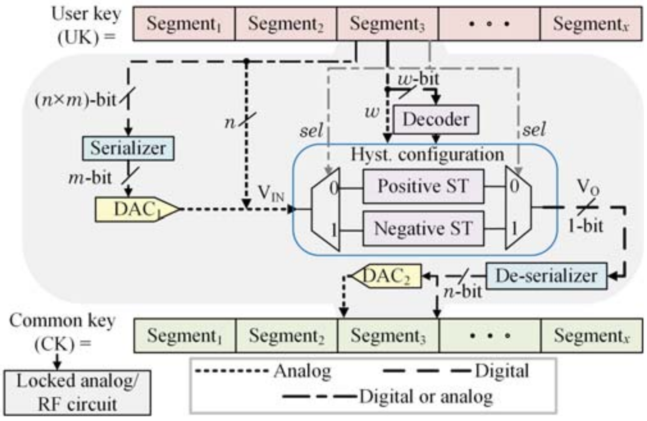


Fig. 7: **Proposed approach.** The UK consists of x segments that reuse the same circuitry. Each segment selects between a positive ST or negative ST, configures the threshold voltages, and also provides the input voltages to generate the required CK. DAC_1 is needed for digital UKs, but not for analog UKs. DAC_2 is needed for analog CKs, but not for digital CKs.

decoder is required to generate the control bits of the digitally programmable resistors. Otherwise, an analog UK includes the control voltages for the T-network resistors implementation, as shown in Fig. 4(c). Also, when the UK is digital, a serializer receives $n \times m$ bits and delivers at the output m-bits at the time. Each m-bits are fed to the digital-to-analog converter (DAC_1) to generate an analog input voltage V_{IN}. Then, V_{IN} is applied to the ST to produce a single-bit output V_O. This process is repeated n times per segment, keeping w fixed, and generating a n-bit segment of the CK. The delays of the serializer, the DAC, the STs and the MUX define the total time required to generate a single bit of the CK.

Finally, this process is repeated for each segment to produce the CK of size $x \times n$ bits. Thus, the size of the search space of the CK is $2^{x \times n}$. The probability of each output outcome is equal to the product of the transition probabilities of all the input values applied serially. Consequently, by dedicating a key-bit per segment sel to select between positive or the negative ST randomly, the distribution of CK becomes closer to a uniform distribution. Although the output key is in the digital domain, the key provisioning can also generate analog CKs by including the DAC_2 shown in Fig. 7.

C. Security metrics

This section discusses the security metrics when both the UK and the CK are digital.

1) Key size

The UK size is dependent on x, w, n, and m, which are the number of segments of the UK, the number of bits configuring the HW, the number of inputs per segment, and the number of bits representing each input, respectively. As illustrated in Fig. 7, the size of the UK is given by $x \times (w + (n \times m) + 1)$. Hence, the possible values of the UK are $2^{x \times (w+(n \times m)+1)}$. As explained in Section III-B, the CK is the concatenation of the output responses of ST from all the segments. Hence, the size of the CK is $x \times n$. The probability of attaining a specific CK is equivalent to the product of the output transition probabilities of the individual segments explained in Section II-B.

Unlike other key provisioning techniques where the circuit size increases as the UK's size increases, our proposed approach does not incur any extra area overhead as the UK's size increases. Any desired size of the UK can be achieved by increasing x or n per x. However, increasing the UK size impacts the chip activation time, i.e., the time taken to generate the CK once the chip is turned on. This time delay is considered non-critical as it is a one-time delay at power-up.

2) Resiliency against brute force attacks

In a brute force attack, the attacker obtains an unlocked chip and use it as an oracle to find the correct UK. He/She explores the whole search space by trial and error or using advanced techniques like optimization algorithms. The robustness of defense approaches to brute force attacks is related to the effort required to find the correct key. Hence, a defense technique is provable secure if the key size is such that the effort required to break it is impractical. A UK size of 80 bits is considered unbreakable trough a brute force attack [9]. Therefore, the UK can be designed such that $x(w + (n \times m) + 1) \geq 80$.

3) Resiliency against reverse engineering attacks

As specified in our threat model described in Section III-A, the attacker can obtain the reverse-engineered netlist of the chip using services such as Chipworks [30]. The extracted netlist includes the key provisioning unit and the locked analog circuit. Even if the attacker can predict the CK from the locked analog circuit using mathematical formulations [15], he/she cannot predict the UK due to:

- The CK ports are not controllable and observable, i.e., the attacker cannot perform internal probing on the CK ports. The only way to control the CK is via the UK.
- The attacker can neither remove nor bypass the key provisioning unit to obtain direct access to the CK ports. As this work assumes resilience only against overproduction, the attacker has the resource only to overproduce the netlist but cannot perform any modifications to the existing netlist.
- Some of the bits configuring the HW are set permanently using on-chip fuses. This information cannot be obtained through reverse engineering techniques.

4) Resiliency against SAT/SMT attacks

The satisfiability-based (SAT) attack is based on Boolean logic. Although the output of the ST is Boolean, its input is a continuous analog voltage. Therefore, a SAT attack cannot be formulated on the proposed key-provisioning circuit. However, satisfiability modulo theories (SMT) can handle non-Boolean variables. In [15], the SMT-based attack was demonstrated successful on breaking most of the existing analog defense techniques. Although, equations of the working of the ST can be easily formulated, the HW configuration bits stored in on-chip fuses are not available to the attacker preventing him/her from formulating the SMT constraints.

5) Probability distribution of the common key (CK)

The effort of finding the correct UK increases as the distribution of the CK approaches a uniform distribution. We quantify how close is the distribution of the CK, provided by the proposed approach, to a uniform one. Also, we analyze the effect of having a non-uniform distribution in the security level. There are several metrics available to measure the randomness of the generated CK. We use the entropy

E as a metric of key unpredictability [31]. The entropy is calculated using Equation (4), where P_i is the probability of each outcome i or value of the CK.

$$E(CK) = \sum_i P_i \cdot log_2 \left(\frac{1}{P_i} \right) \tag{4}$$

If the probability of a single-bit taking the value ‘0’ or ‘1’ is equal, $P(0)$=$P(1)$=0.5, the entropy equals the number of bits, one in this case. Otherwise, if $P(0) \neq P(1)$, the bit does not have a random distribution, and the entropy is smaller than one-bit. Hence, the entropy also determines the effective key size.

6) *Uniqueness of the user key (UK)*

In the case an attacker manages to find the correct UK of a chip, he/she should not be able to unlock other chip instances using this UK. Hence, each chip should have a unique UK value. This security property imposes two restrictions:

- The correct UKs of two different chips producing the same CK should be statistically different.
- The correct UK of one chip should not activate another chip.

To address the first restriction, we use the Hamming distance metric. The Hamming distance between two binary numbers is defined as the number of bit positions at which their values differ. The key provisioning unit should be designed such that several UKs that produce the same CK have a Hamming distance equivalent to 50% of the UK’s size.

The second restriction is met by hardcoding certain bits of the HW configuration using on-chip fuses. These fuses are written by the IP owner in a trusted facility after fabrication. These fuse settings ensure a unique configuration of the threshold voltages for each chip. Thus, two key provisioning units having different HW configurations generate different CKs for the same UK. Moreover, to generate the same CK with different HW configurations, the UKs must be different.

IV. Results and discussion

A. *Experimental setup*

The transistor-level circuit simulations of our proposed ST-based key provisioning technique are performed using the Spectre® simulation platform. This technique is implemented using the IBM 180 nm CMOS process with a 1.8 V supply. Each DAC is built using the R-2R DAC topology [32]. Also, integrated polysilicon resistors realize the programmable resistors. The serializer/de-serializer is coded using Verilog HDL and is synthesized using the chosen CMOS process. The security metrics, such as the uniqueness of the UK and the effective CK’s size, are determined from the behavioral model of the key provisioning unit implemented using MatLab®.

B. *Effective size of the common key (CK)*

The following experiment calculates the entropy of the CK generated by the proposed technique in response to a single UK’s segment ($x = 1$). This experiment is repeated for different combinations of w, m, and n. The resolution of the threshold voltages and the input voltage depends on w and m, respectively. We evaluate the outputs of all the possible combinations of HW settings, input voltage values, and the type of the ST (positive or negative hysteresis). Then, we calculate P_i, the probability of each output value i.

The entropy of the CK is calculated using Equation (4). Table II lists the entropy for different combinations of w, m, and n. If the CK generated by the key provisioning unit has a uniform distribution, the calculated entropy equals n, which is the number of inputs applied sequentially. Hence, the closer the value of entropy approaches n, the closer is the distribution of CK to the uniform distribution. The entropy thus quantifies the effective number of information bits of the CK.

TABLE II: The entropy of the CK for all combinations of w, n, and m. w bits set the width of the HW. n is the number of m-bit input values applied in series.

$\boldsymbol{w}$	**2**			**3**			**4**		
$\boldsymbol{m}$ \ $\boldsymbol{n}$	**3**	**4**	**5**	**3**	**4**	**5**	**3**	**4**	**5**
2	2.97	3.93	4.87	2.97	3.93	4.87	2.97	3.93	4.87
3	2.96	3.89	4.81	2.95	3.87	4.77	2.95	3.89	4.80
4	2.93	3.84	4.72	2.95	3.88	4.78	2.95	3.87	4.77

From the results in Table II, the effective key size (entropy) is smaller than the actual key size (n). However, the degradation in the effective key size is less than one bit. This information is useful for designing the ST-based key provisioning unit. For example, consider $w = m = 4$, and the desired number of bits of CK is 4. Selecting $n = 4$ translates to only 3.87 bits of CK that is insufficient. Therefore, $n = 5$ is chosen to achieve the desired level of security.

We extrapolated the results of this experiment to estimate the effective key size of larger CKs. Fig. 8 shows the discrepancy between the effective size of a key generated with a TRNG and the proposed technique under different configurations. We estimated the effective key size for static or dynamic HW, and only positive ST (PST) or positive and negative ST (PST & NST). In all cases, the HW is centered at the middle of the supply voltage. The CK’s entropy is highly dependent on the threshold values. In a static configuration, the smaller the HW, the larger the entropy. The effective key size of the dynamic hysteresis configuration considers all possible hysteresis widths. For instance, Fig. 8 shows the effective key calculated for a static configuration with a 0.4V HW versus a dynamic window with $w = m = 4$. Although a static configuration can have higher entropy than a dynamic one, it is a weak approach since it reduces the attacker’s effort to find the correct key. Moreover, having both PST and NST increases the effective key size compared with using a PST alone, at

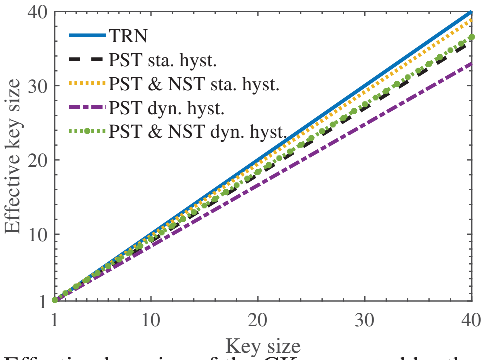


Fig. 8: Effective key size of the CK generated by the proposed key provisioning compared to a true number (TRN). The effective CK’s size is calculated when the hysteresis window (HW) is static or dynamic and using a positive ST (PST) alone or combined with a negative ST (NST).

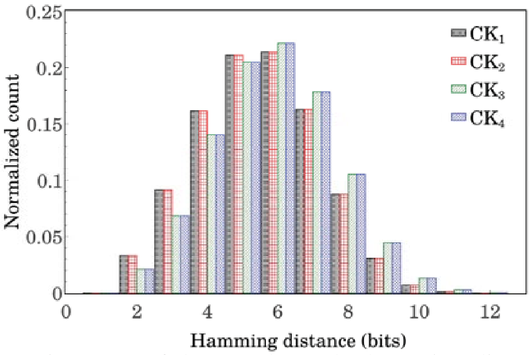


Fig. 9: Uniqueness of the user key. The hamming distance of all user keys is calculated for different common keys CK_1, CK_2, CK_3, and CK_4.

the expense of extra area. This experiment demonstrates that a dynamic HW with PST & NST is a good design for increasing the security level.

C. Uniqueness of the user key (UK)

We calculate the Hamming distances between each UK and the other UKs that generate the same CK to determine their uniqueness. For instance, in a ST-based key provisioning unit with $x = 1$, $w = 2$, $m = 2$, and $n = 5$, the size of UK and CK equals 13 bits and 5 bits, respectively. Due to the probability distribution of the CK, there are $\approx 2^{13}/2^5$ distinct UKs that produce the same CK. We calculate the Hamming distance between all the possible values of UKs generating the same CK. The experiment is repeated for all the values of CK. Fig. 9 shows a histogram of the Hamming distances between the UKs for four different CKs. This plot follows a Gaussian response, where the mean Hamming distance between UKs is equal to 6 bits, i.e., approximately equal to 50% of the UK's size (13 bits).

D. Power and area overhead

The ST-based key provisioning unit consumes power only during a short period at power-up. During this time, the circuit acquires the UK and generates the corresponding CK. Then, the CK is stored in a shift register, applied to the locked circuit, and the key-provisioning unit is powered down. Therefore, **there is no power consumption during runtime** [8].

However, the key provisioning circuit is integrated on-chip and incurs an area overhead. The area overhead is calculated for different variations of the proposed approach, depending on the ST's circuit topology and whether it uses analog or digital keys. The positive and negative STs can be implemented either with internal or external feedback (Fig. 4 and Fig. 5), yielding different area overheads.

As the proposed approach is compatible with both digital and analog keys, the area overhead of each configuration accounts for the implementation of all required circuit blocks, according to Fig. 7. Hence, the integrated area in Table III includes the positive ST, the window comparator, the MUX for selection, the programmable resistors, the decoder (5-bit decoder for digital UKs only), the serializer, DAC_1 (5-bit DAC for digital UKs only), the de-serializer, and DAC_2 (5-bit DAC for analog CKs only). All this circuitry is required to process one key segment at the time. Hence, the circuit is reused for the x segments that form the UK. Moreover, increasing the UK size can be done by increasing x without any change in the circuit implementation.

TABLE III: Area overhead of the ST-based key provisioning implementation for keys in the digital or the analog domain.

User key	Common key	Internal feedback ST [mm^2]	External feedback ST [mm^2]
Digital	Digital	0.010	0.014
Digital	Analog	0.013	0.017
Analog	Digital	0.001	0.003
Analog	Analog	0.004	0.005

We also compare the area overhead of our approach with other key-provisioning techniques when both the UK and the CK are digital. Table IV summarizes the comparison. The area of the previous works is not reported for these key sizes but estimated from their reported results [2, 7–9]. In [2], generating a 64-bit key incurs in an area overhead given by a TRNG and the RSA core implementation [2]. While the integrated area of the TRNG is 0.036mm^2 in a 130 nm process, the RSA requires around 10,000 two-input gates. These numbers were scaled to the 180 nm process for comparison. In [7], the circuit overhead is given by the PUF and digital circuitry. Its area was estimated from the reported results of three different circuits implemented in the 180 nm process, with different key sizes. In [9], the area of the neural-network-based key provisioning is not reported. However, it can be estimated from the picture of the experimental setup. AMSlock [23] is not included in the comparison because its operation differs from a key provisioning technique.

From the comparison in Table IV, we observe that **the proposed approach has the best area efficiency than all the other techniques** for all the key sizes. In contrast with the PUF-based key generation, in the proposed approach, **the area efficiency increases with an increase in the key size**.

Another aspect of the overhead is the execution time. The time required for the generation of each CK's segment includes the configuration time t_1 and the evaluation time t_2. The HW is set during t_1. During t_2, the ST receives a sequence of n inputs and generates the corresponding outputs. Hence, the total time t_t is a product of the time per segment and the number of segments $t_t = x \times (t_1 + t_2)$. On average, it takes t_t=1.8μs to produce an 80-bit CK.

E. Robustness against process and temperature variations

Since the HW is represented by w bits, the threshold values are not continuous but discrete. The resolution step is given by $(V_{DD} - V_{SS})/(2^w)$. On top of that value, process and temperature variations can modify the threshold values. The proposed approach is considered robust to variations if the deviation caused by them is small compared with the resolution step of the thresholds.

A 1000-sample Monte Carlo simulation was performed to estimate the variation in the threshold voltages due to process and temperature variations. V_{TH} variations are smaller than

TABLE IV: Area overhead comparison with other techniques.

UK size [bits]	EPIC [2] [mm^2]	PUF ID XOR UK [7][mm^2]	Analog NN [9] [mm^2]	This work [mm^2]
80	0.282	0.017	>100	0.014
128	0.282	0.027	>100	0.014
256	0.282	0.054	>100	0.014

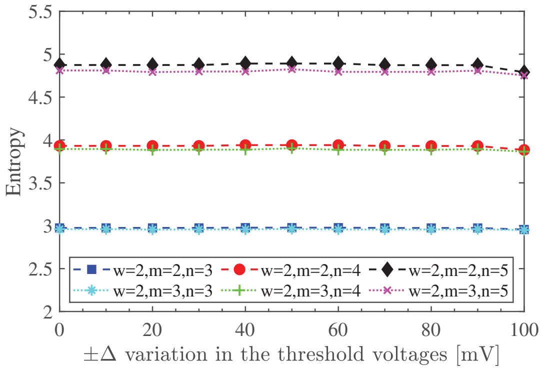


Fig. 10: Estimated variation on the common key's entropy due to a ±Δ voltage variation in V_{TL} and V_{TH}. The results of six experiments with different values of the number of bits describing the hysteresis window w, the input values m, and the number of inputs n are reported.

3×7.455 mV based on a 1000-sample Monte-Carlo simulation results from -40° C to 85° C. As the output voltage saturates to either higher or lower supply voltage, the output of the ST is insensitive to voltage variations. **Hence, it does not incur any performance degradation**.

We also evaluated the impact of variations on the distribution of the CK. Fig. 10. The entropy was calculated for various combinations of w, m, and n similar to the results reported on Table II. However, in this experiment, both thresholds have an additional ±Δ error. The results demonstrate a worst-case degradation of 0.1-bit for as much as a 100 mV error in the threshold voltages. It is around $5X$ the $\pm 3\sigma$ variation estimated due to process and temperature changes.

F. Test cases with analog locks

The proposed key provisioning approach is demonstrated on three different locked analog/RF IC designs. They represent three broad areas of application. An active filter, used in signal processing [33]; a low-dropout (LDO) voltage regulator used in power management [34]; and a low noise amplifier, a fundamental block in RF receivers [35]. All the circuits were implemented using the IBM 180 nm process and powered by a 1.8 V supply. We simulated each circuit's performance when applied: i) the correct UK, and ii) several incorrect UKs.

1) Bandpass fourth-order Gm-C filter

A 4^{th} order Gm-C filter is implemented as a cascade of two 2^{nd} order filters. The circuit schematic of a 2^{th} order Gm-C filter is presented in Fig. 11. Its transfer function is

$$H_{BPF} = \frac{V_{out}}{V_{in}} = \frac{g_{m1}C_1 s}{s^2 C_1 C_2 + s g_{m3} C_2 + g_{m2} g_{m4}}. \quad (5)$$

The performance metrics of the filter are center frequency $\omega_o = \sqrt{\frac{g_{m2}g_{m4}}{C_1 C_2}}$, quality factor $Q = \frac{1}{g_{m3}}\sqrt{\frac{g_{m2}g_{m4}C_1}{C_2}}$, gain of the passband $H(j\omega_o) = \frac{g_{m1}C_1}{g_{m3}C_2}$, and bandwidth $BW = (\omega_o/Q)$ [33]. The bias current to each OTA is provided by a non-monotonic, non-concave configurable current mirror (CCM) based lock [7]. Each CCM-lock is controlled by 12 bits. Hence, the total size of the CK is 96 bits. The ST-based key provisioning block is designed with $x = 12$, $n = 8$, $w = 5$ and $m = 5$ to produce the CK of size 96 bits. Also, the size of the UK is 552 bits. As illustrated in Fig. 12, the correct key sets the performance metrics of the filter equal to the desired values, i.e., $f_o = \omega_o/(2\pi)$=268 kHz, BW=154 kHz, and $H(j\omega_o)$=0 dB. For the incorrect keys, as shown in the figure, the circuit specification is not met.

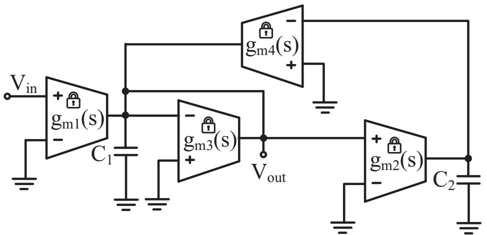


Fig. 11: Second order Gm-C bandpass filter.

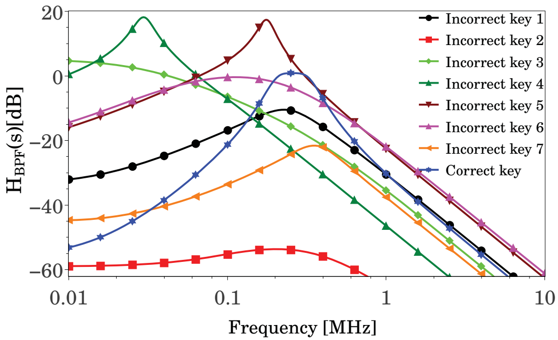


Fig. 12: Transfer function of 4th order Gm-C filter for the correct and incorrect keys. The specifications of the filter are met only for the correct key.

2) Low-dropout (LDO) voltage regulator

A capacitor-less LDO voltage regulator with a single-stage error amplifier [34] is locked with an 18-bit CK. The key controls the biasing of the error amplifier by CCM-based lock and a configurable capacitor bank. The LDO is designed for an input voltage V_{in}=1.8 V and an output voltage V_{out}=1.6 V, resulting in a dropout voltage of 200 mV. This LDO is designed to provide a stable output voltage under the load conditions I_L=(100 μA, 20 mA), with a load capacitor C_L=1 nF.

The 18-bit CK is produced by the ST-based key provisioning with the following configuration, $w = 5$, $m = 5$, $n = 3$, and $x = 6$. This lock secures two fundamental performance metrics of LDO: the phase margin $PM > 45°$ and the power supply rejection $PSR(@1KHz)$ >70 dB. As illustrated in Fig. 13

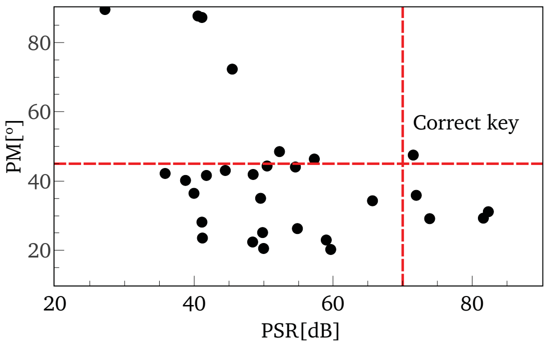


Fig. 13: Applying the correct key to the locked LDO, gives the desired performance $PM > 45°$ and PSR >70 dB, whereas an incorrect key gives undesired performance.

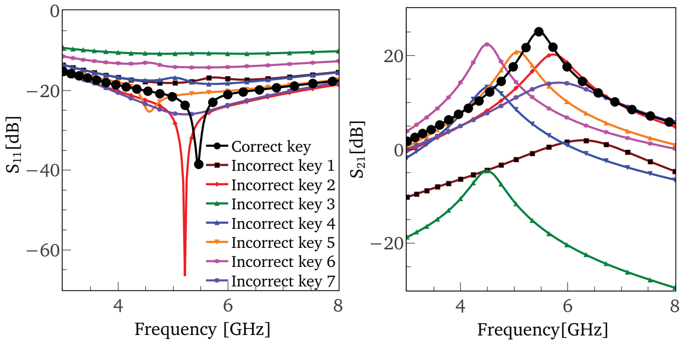


Fig. 14: S_{11} ≤-30 dB and S_{21} >25 dB when correct key is applied to the locked LNA. Otherwise, for an incorrect key, the S-parameters do not satisfy the specifications.

the LDO's performance metrics meet the specifications across the given current load range for the correct key. However, for an incorrect key, the measured PM and PSR do not meet the design specifications.

3) *Cascode common-gate low-noise amplifier (CG-LNA)*

The cascode CG-LNA is a popular LNA topology [35]. In this circuit, a 24-bit CK controls the CCM providing the bias current of the gain transistor and the configurable tank load. The ST-based key provisioning block is configured with $w = 5$, $m = 5$, $n = 6$, and $x = 4$. Thus, the size of the UK is 184 bits. The circuit specifications of the secured cascode CG-LNA are input matching S_{11} <-30 dB and gain S_{21} >25 dB. Fig. 14 shows the impact of the correct and incorrect UKs on the performance of the CG-LNA. Only the correct key gives the desired performance of S_{11}=-39 dB and S_{21}=26 dB.

4) *Overhead of the key provisioning on the test cases*

The area overhead and the energy consumption of the proposed ST key are reported in Table V. The area overhead is compared with the original area of the locked analog circuit, and it includes the elements of Fig. 7(d): serializer, DAC, ST, window comparator, MUX, decoder, programmable resistors, and de-serializer.

From Table V, we observe that for analog/RF circuits with an area larger than 0.5 mm^2, the overhead is smaller than 3%. As expected, the area overhead is more considerable for smaller circuits like the LDO. However, the LDO is often integrated to provide a stable voltage to other circuits in a larger architecture. Hence, a locked LDO enables the IP protection of different circuit blocks by controlling their supply voltages and reducing the area overhead of our approach.

V. Related works on Analog/RF locking

Analog/RF locking has been leveraged from digital logic locking. Logic locking is one of the preferred DfTr techniques, as it secures the design from the attacker present anywhere in the supply chain. In analog locking, the circuit performance is locked and is made available only to the authorized user. The following section discusses the several analog locking techniques proposed by the researchers.

TABLE V: The area overhead incurred by the proposed key provisioning unit on different locked analog circuits.

Circuit under test	UK size [bits]	CK size [bits]	Original Area [mm^2]	Area overhead		Energy [nJ]
				Area [mm^2]	Pct. %	
GM-C BPF	552	96	0.692	0.014	2.02	13.35
LDO	126	18	0.163	0.014	8.58	2.53
LNA	144	24	0.724	0.014	1.93	3.35

A memristor-based voltage divider circuit biases the bulk terminals of the differential pair of sense amplifiers [6]. An incorrect key does not compensate for the offset voltage, thereby affecting the sensitivity and reliability of the sense amplifiers. The combinational lock technique [7] locks the current biasing using CCMs. Only the correct key configures the current mirror to provide the desired bias to the circuit under protection. Otherwise, an incorrect key gives a bias current outside the acceptable range. Similar to [7], the effective width of the transistor depends on the key inputs in parameter biasing obfuscation technique [10]. The key inputs determine the required bias. In [13], the design locking is extended to the transistor sizing by implementing critical transistors in a mesh configuration that has an equivalent composite transistor.

Researchers have also proposed locking techniques for protecting mixed-signal circuits (AMS) [8, 11]. These techniques lock the digital section of the AMS circuits. Only the correct key can set the specifications of the analog/RF circuits to the desired values. An incorrect key sets one or more specifications of the analog/RF circuit outside the acceptable range. Both the analog and digital sections of the AMS circuits are locked [12]. In [9], a locked analog neural network generates the bias voltage for the RF circuit.

In all the above locking techniques, except for the combinational lock [7], all chip instances of the given design are protected using the same key. If an attacker determines this key using mathematical modelling [15], he/she can unlock all the chip instances. Hence, integrating our key provisioning technique along with the existing locking techniques ensures that if the attacker determines the key for one chip instance, he/she cannot use the same key to unlock other chips. This integration also adds the following advantages to the locked design: (i) The locking technique will not require a large input key (CK) size to have a sufficient security level. Instead, that requirement is transferred to the UK. It reduces the area overhead of the analog lock, compared with the original circuit. (ii) The integrated key provisioning unit increases the effort of brute force and reverse engineering attacks. (iii) Our key provisioning unit is resilient to process and temperature variations and has a small area overhead.

VI. Conclusion

An ST-based key provisioning circuit has been designed and characterized for the security metrics considered. Our approach leverages a highly configurable circuit based on hysteresis comparators for a high resiliency to overproduction attacks. Increasing the sizes of both the CK and the UK is done by reusing the integrated circuitry. Hence, compared to the previous key provisioning techniques, the proposed techniques incur lesser area overhead. It takes approximately $\frac{1}{20.1}$ times the size of [2], half the size of [7], and $\frac{1}{7142}$ times the size of [9]. The proposed key provisioning only consumes power at the power-up time. Therefore, power overhead is not a concern for our approach. The chip activation time increases with the key size. The proposed method takes on average $1.8\mu s$ to acquire the UK and generate an 80-bit CK. This delay occurs during the power-up.

The IP rights holder designs the security metrics of this approach through the circuit settings. Experimental results demonstrate the efficacy of this approach on securing the performance of analog/RF circuits for both digital and analog keys. PVT variations do not affect the entropy of the generated key. Additional settings for the tuning of the center of the HW can be studied to increase the entropy of the CK further. Moreover, enabling a dynamic segment length could increase the resilience to brute force attacks.

Acknowledgement

This work is funded by National Science Foundation (CCF-1815583). Also, this work is partially funded by Silicon Labs, Qualcomm, and Texas Instruments.

References

[1] M. Rostami, F. Koushanfar, and R. Karri, “A Primer on Hardware Security: Models, Methods, and Metrics,” *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1283–1295, 2014.

[2] J. A. Roy, F. Koushanfar, and I. L. Markov, “Ending Piracy of Integrated Circuits,” *Computer*, vol. 43, no. 10, pp. 30–38, 2010.

[3] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, “Security Analysis of Logic Obfuscation,” *ACM/IEEE Design Automation Conference*, pp. 83–89, 2012.

[4] Y. Xie and A. Srivastava, “Mitigating SAT Attack on Logic Locking,” *Cryptographic Hardware and Embedded Systems*, pp. 127–146, 2016.

[5] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. J. Rajendran, and O. Sinanoglu, “Provably-Secure Logic Locking: From Theory To Practice,” *ACM SIGSAC Conference on Computer & Communications Security*, pp. 1601–1618, 2017.

[6] D. H. K. Hoe, J. Rajendran, and R. Karri, “Towards Secure Analog Designs: A Secure Sense Amplifier Using Memristors,” *IEEE Computer Society Annual Symposium on VLSI*, pp. 516–521, 2014.

[7] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sánchez-Sinencio, and J. Hu, “Thwarting Analog IC Piracy via Combinational Locking,” *IEEE International Test Conference*, pp. 1–10, 2017.

[8] N. G. Jayasankaran, A. Sanabria-Borbón, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, “Towards Provably-Secure Analog and Mixed-signal Locking Against Overproduction,” *IEEE/ACM International Conference on Computer-Aided Design*, pp. 7:1–7:8, 2018.

[9] G. Volanis, Y. Lu, S. G. R. Nimmalapudi, A. Antonopoulos, A. Marshall, and Y. Makris, “Analog Performance Locking through Neural Network-Based Biasing,” *VLSI Test Symposium*, pp. 1–6, 2019.

[10] V. V. Rao and I. Savidis, “Protecting Analog Circuits with Parameter Biasing Obfuscation,” *IEEE Latin American Test Symposium*, pp. 1–6, 2017.

[11] J. Leonhard, M. Yasin, S. Turk, M. T. Nabeel, M.-M. Louërat, R. Chotin-Avot, H. Aboushad, O. Sinanoglu, and H.-G. Stratigopoulos, “MixLock: Securing Mixed-Signal Circuits via Logic Locking,” *IEEE/ACM Design Automation and Test in Europe*, 2019.

[12] K. Juretus, V. Venugopal Rao, and I. Savidis, “Securing Analog Mixed-Signal Integrated Circuits Through Shared Dependencies,” *Great Lakes Symposium on VLSI*, pp. 483–488, 2019.

[13] V. V. Rao and I. Savidis, “Mesh Based Obfuscation of Analog Circuit Properties,” *IEEE International Symposium on Circuits and Systems*, pp. 1–5, 2019.

[14] P. Subramanyan, S. Ray, and S. Malik, “Evaluating the Security of Logic Encryption Algorithms,” *IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 137–143, 2015.

[15] N. G. Jayasankaran, A. Sanabria-Borbn, A. Abuellil, E. Snchez-Sinencio, J. Hu, and J. Rajendran, “Breaking analog locking techniques,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, pp. 1–14, 2020.

[16] M. Yasin, S. M. Saeed, J. Rajendran, and O. Sinanoglu, “Activation of Logic Encrypted Chips: Pre-test or Post-Test?” *IEEE/ACM Design, Automation & Test in Europe*, pp. 139–144, 2016.

[17] S. Lin, Y. Cao, X. Zhao, X. Wang, and X. Pan, “A Compact Ultra-low Power Physical Unclonable Function Based on Time-Domain Current Difference Measurement,” *IEEE International Symposium on Circuits and Systems*, pp. 277–280, 2016.

[18] Z. Paral and S. Devadas, “Reliable and Efficient PUF-Based Key Generation Using Pattern Matching,” *IEEE International Symposium on Hardware Oriented Security and Trust*, no. 978, pp. 128–133, 2011.

[19] M. Khalafalla and C. Gebotys, “PUFs Deep Attacks: Enhanced Modeling Attacks Using Deep Learning Techniques to Break the Security of Double Arbiter PUFs,” *Design, Automation Test in Europe Conference Exhibition*, pp. 204–209, 2019.

[20] J. Delvaux, “Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUFFSMs,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2043–2058, 2019.

[21] C. W. Lin and S. Ghosh, “A Family of Schmitt-Trigger-Based Arbiter-PUFs and Selective Challenge-Pruning for Robustness and Quality,” *IEEE International Symposium on Hardware Oriented Security and Trust*, pp. 32–37, 2015.

[22] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sanchez-Sinencio, and J. Hu, “Thwarting Analog IC Piracy via Combinational Locking,” *IEEE International Test Conference*, pp. 1–10, 2017.

[23] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, “Towards Provably-Secure Analog and Mixed-Signal Locking Against Overproduction,” *IEEE/ACM International Conference on Computer-Aided Design*, pp. 7:1–7:8, 2018.

[24] J. Leonhard, M.-M. Louërat, H. Aboushady, O. Sinanoglu, and H.-G. Stratigopoulos, “Mixed-Signal Hardware Security Using MixLock: Demonstration in an Audio Application,” *International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design*, pp. 185–188, 2019.

[25] S. Franco, *Design with Operational Amplifiers and Analog Integrated Circuits*. McGraw-Hill, Inc., 2015.

[26] A. Pfister, “Novel CMOS Schmitt Trigger with Controllable Hysteresis,” *Electronics Letters*, vol. 28, no. 7, pp. 639–641, 1992.

[27] P. E. Allen and D. R. Holberg, *CMOS Analog Circuit Design*. Oxford University Press, 2002.

[28] B. L. Dokic, “CMOS Schmitt Triggers.” *IEE Proceedings, Part G: Electronic Circuits and Systems*, vol. 131, no. 5, pp. 197–202, 1984.

[29] C.-K. Pham, “CMOS Schmitt Trigger Circuit with Controllable Hysteresis Using Logical Threshold Voltage Control Circuit,” *IEEE/ACIS International Conference on Computer and Information Science*, pp. 48–53, 2007.

[30] Chipworks, “Reverse engineering software,” https://www.techinsights.com/, 2016, Last accessed on 04/29/2020.

[31] M. Alioto, “Trends in Hardware Security: From Basics to ASICs,” *IEEE Solid-State Circuits Magazine*, vol. 11, no. 3, pp. 56–74, 2019.

[32] B. Greenley, R. Veith, D. Y. Chang, and U. K. Moon, “A Low-Voltage 10-Bit CMOS DAC in $0.01-mm^2$ Die Area,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 52, no. 5, pp. 246–250, 2005.

[33] R. Schaumann, H. Xiao, and V. V. Mac, *Design of Analog Filters*. Oxford University Press, Inc., 2009.

[34] S. Hong and G. Cho, “High-Gain Wide-Bandwidth Capacitor-Less Low-Dropout Regulator (LDO) for Mobile Applications Utilizing Frequency Response of Multiple Feedback Loops,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 1, pp. 46–57, 2016.

[35] B. Razavi, *RF Microelectronics*. Pearson Education, 2011.