RF Transceiver Security Against Piracy Attacks

Alán Rodrigo Díaz Rizo, Julian Leonhard, Hassan Aboushady, Haralampos-G. Stratigopoulos

RF Transceiver Security Against Piracy Attacks

Alán Rodrigo Díaz Rizo, Julian Leonhard, Hassan Aboushady, *Senior Member, IEEE*, and Haralampos-G. Stratigopoulos, *Member, IEEE*

***Abstract*—We demonstrate for the first time system-level locking for RF transceivers serving as an anti-piracy security technique. The locking strategy is to make RF performance key-dependent by leveraging a state-of-the-art logic locking technique to obfuscate digital blocks in the signal path. The technique presents several advantages, including general applicability, effective locking for incorrect keys, attack resilience, transparency when the correct key is used, minimum overheads, and ease of implementation. We show that logic locking cannot be blindly applied in this context and, in this regard, we show how it can be adapted towards effective RF transceiver locking. A proof-of-concept is demonstrated with hardware measurements.**

***Index Terms*—Hardware security and trust, IP/IC piracy, locking, RF transceivers.**

I. Introduction

The globalisation of the Integrated Circuit (IC) design and manufacturing flow leaves ICs unprotected against piracy attacks [1]. A design house that purchases a licence for using a third-party Intellectual Property (IP) block (3PIP), the foundry that is subcontracted for fabricating the IC, and an end-user who has capabilities for reverse-engineering a legally purchased chip, can easily clone the complete IP/IC or part of it without the consent or knowledge of the IP/IC owner, thus resulting in know-how, competitive advantage, and financial losses for the IP/IC owner. Beyond cloning, other piracy attacks include chip overbuilding by the foundry, remarking out-of-spec chips by the test facility, and chip recycling [1].

An end-to-end protection against IP/IC piracy is locking. It is carried out by the IP/IC owner and aims at transforming the circuit function $O = F(I)$, where I and O denote input and output, respectively, to a new function $O = F_l(I, K)$, where K is a key, typically in the form of a large bitstring. There is a single key k_{corr} that unlocks the circuit establishing correct functionality, i.e., $F(I) = F_l(I, K)|_{K=k_{corr}}$, $\forall I$. Any other key is incorrect and corrupts the output for some inputs, i.e., $\exists I\, F(I) \neq F_l(I, K)|_{K \neq k_{corr}}$. k_{corr} is the IP/IC owner's secret and is not shared with any untrusted party. It is securely loaded in an on-chip Tamper-Proof Memory (TPM) after chip fabrication, thus thwarting piracy during the design, fabrication, and testing stages, as well as piracy via reverse engineering since any attempt to read the TPM results in irreversible loss of k_{corr}.

Locking was first proposed for digital ICs [2], a.k.a. logic locking. Since then there has been a "ping-pong game" between "defenders" proposing logic locking defenses and "attackers" proposing counterattacks that break them [3].

This paper makes three main contributions:

1) We demonstrate for the first time locking of entire RF transceivers at system-level. The proposed locking strategy makes RF performance key-dependent by leveraging a state-of-the-art logic locking technique, namely Stripped Functionality Logic Locking (SFLL)-rem [4], to obfuscate essential digital blocks in the RF transceiver signal path.

2) We show that logic locking in general cannot be blindly applied to Analog/Mixed-Signal (A/M-S) ICs. To this end, we show how SFLL-rem can be tuned in the context of RF transceiver locking.

3) A proof-of-concept is demonstrated with hardware measurements using the Software Defined Radio (SDR) bladeRF board from Nuand™.

Locking an A/M-S IC via logic locking of its digital section has been demonstrated in the past for individual A/M-S IC blocks [5]–[7]. One possibility is to perform logic locking of the digital processor of the feedback calibration loop of A/M-S ICs [7]. Herein, we demonstrate locking of entire RF transceivers at system-level.

Other A/M-S IC locking approaches include biasing locking [8]–[11], limiting the calibration range [12], and using programming bits as secret keys [13], [14]. Efficient counter-attacks have been proposed for biasing locking [15]–[18], thus this approach is no longer considered secured. The approach in [12] requires floating-gate transistors which are rarely used. The approaches in [13], [14] apply only when multi-bit programmability is in place and assume that the calibration algorithm is unique and unknown to the attacker. A review of anti-piracy solutions for A/M-S ICs is provided in [19].

The remainder of this article is organized as follows. In Section II, we present the proposed RF transceiver locking strategy. In Section III, we provide an overview of SFLL-rem. In Section IV, we show how SFLL-rem is tuned for RF transceiver locking. In Section V, we discuss the resilience to foreseen counterattacks. In Section VI, we present the experimental results. Section VII concludes this article.

II. RF transceiver locking strategy

The proposed locking strategy targets the interaction between analog and digital blocks in the RF transceiver. The

Manuscript received November 15, 2021; revised February 23, 2022; accepted March 28, 2022. This work was supported by the ANR STEALTH project under Grant ANR-17-CE24-0022-01. The work of J. Leonhard was supported by the Doctoral School EDITE de Paris through Fellowship. The work of A. R. Díaz Rizo was supported by the Mexican National Council for Science and Technology (CONACYT) through Fellowship. This article was recommended by Associate Editor J. Goes. (Corresponding author: Haralampos-G. Stratigopoulos.)

Alán Rodrigo Díaz Rizo, Julian Leonhard, Hassan Aboushady, and Haralampos-G. Stratigopoulos are with the Sorbonne Université, CNRS, LIP6, 75005 Paris, France (e-mail: alan-rodrigo.diaz-rizo@lip6.fr; julian.leonhard@lip6.fr; hassan.aboushady@lip6.fr; haralampos.stratigopoulos@lip6.fr).

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2022.XXXXXXX

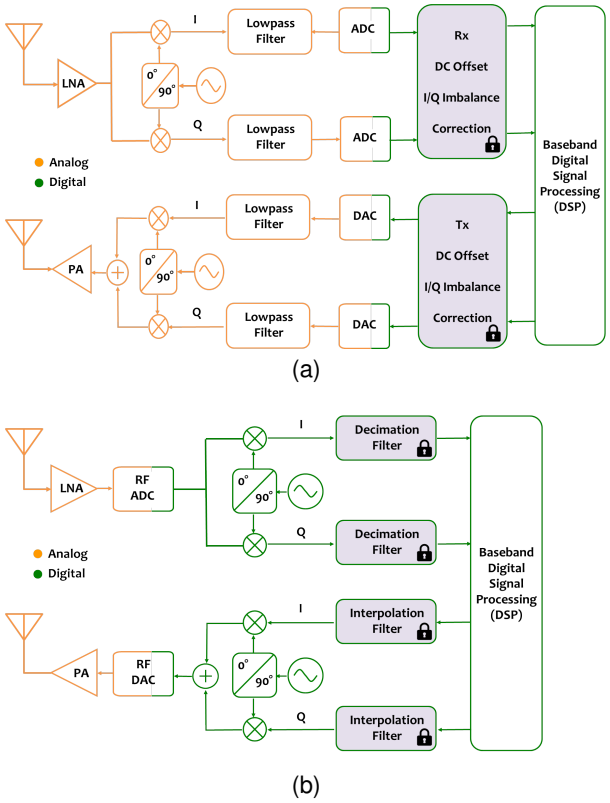

Fig. 1: Main RF transceiver architectures showing the most suitable digital block to lock: (a) conventional; (b) highly-digitized.

underlying idea is to corrupt analog information propagation by performing logic locking in digital blocks in the signal path. In this way, system-level RF performances, e.g., Bit Error Rate (BER), are corrupted in a complex and unpredictable way.

Considering the conventional Zero Intermediate Frequency (Zero-IF) and Low Intermediate Frequency (Low-IF) RF transceiver architectures in Fig. 1a, we can target locking the digital DC Offset (DCO) and I/Q Imbalance (IQI) correction blocks of both the transmitter and the receiver. Considering the highly-digitized RF transceiver architectures in Fig. 1b [20], we can target locking the digital decimation filter in the receiver and the digital interpolation filter in the transmitter. In this paper, we demonstrate with hardware measurements the locked RF transceiver architecture in Fig. 1a.

The locking strategy presents the following advantages:

1) General applicability: It is applicable to any RF transceiver architecture and independent of the complex-valued modulation scheme and constellation size.

2) Locking effectiveness: Only one key unlocks functionality while any incorrect key results in drastic performance degradation.

3) Attack resilience: It generates a large-size digital key, which is a prerequisite for achieving resiliency against counterattacks. It also borrows and capitalizes on the security properties of state-of-the-art logic locking mechanisms to provide strong security against counterattacks.

4) Transparency: There is no performance penalty since (a) analog blocks are left intact and (b) advanced logic locking techniques intentionally do not modify critical paths in the digital section, thus the delay penalty if any is practically negligible having no effect on RF performance.

5) Minimum overheads: The small and justifiable area and power overheads for the digital blocks resulting from the locking operation become negligible when projected to the entire RF transceiver.

6) Ease of implementation: The A/M-S design flow does not change and no A/M-S block needs to be re-designed. The locking step can be seamlessly integrated into the digital design flow since logic locking is automated [3].

III. Logic Locking with SFLL-rem

The steps of SFLL-rem [4] are summarized below:

1) Perform a stuck-at fault injection campaign on the original circuit F. A stuck-at fault means tying a net to a constant logical 0 (i.e., ground) or 1 (i.e., V_{DD}).

2) For each injected fault we record the input test patterns that detect the fault, i.e., the fault effect propagates to the output resulting in a flipped output bit. These input test patterns are called *failing input test patterns* and their set is denoted by T_f.

3) The fault injection campaign does not have to be exhaustive; it suffices to find a fault f that has a failing input test pattern with k care bits and $n-k$ don't care bits, where n is the number of inputs. This failing input test pattern is denoted by t_{secure} and, in essence, represents a total of 2^{n-k} failing input test patterns. These 2^{n-k} failing input test patterns are called *protected input patterns (PIPs)*.

4) We select the k care bits of t_{secure} to be the secret key k_{corr} of size k.

5) Due to the injection of fault f, F is transformed to circuit F_f. Some internal nets now being tied high or low, allows us to remove logic and simplify F_f with regard to F. Compared to F, F_f produces an erroneous output for the complete set T_f of failing input test patterns.

6) Redesign F_f by adding logic to restore the functionality for all failing input test patterns in the set $\{T_f - t_{secure}\}$, resulting in circuit $F_{f'}$. Compared to F, $F_{f'}$ produces an erroneous output only for the PIPs represented by t_{secure}.

7) Generate the target circuit F_l from $F_{f'}$ by adding to $F_{f'}$ a restore unit and a 2-input XOR gate. Specifically, let $I^{'}$ be the concatenation of input bits whose positions map to the positions of the care bits of t_{secure} that compose the secret key k_{corr}. The restore unit implements a generic comparison function based on a look-up operation comparing $I^{'}$ to the key k_{corr} stored in the TPM. The output of the restore unit is 1 when $I^{'} = k_{corr}$ and 0 when $I^{'} \neq k_{corr}$. The XOR gate is driven by the output O and the output of the restore unit, and the output of the XOR gate is the output of F_l. In this way, we correct functionality for the remaining 2^{n-k} PIPs represented by t_{secure}. If an invalid key k_{corr} is used, then correction fails.

IV. SFLL-rem tuned for RF transceiver locking

Herein, we show how SFLL-rem is tuned for RF transceiver locking considering the architecture in Fig. 1a. SFLL-rem is applied to the DCO-IQI correction blocks. The pseudo-algorithm is shown in Algorithm 1 where F is the DCO-IQI

Algorithm 1 SFLL-rem tuned for RF transceiver locking

Input: Original circuit netlist F
Output: Locked circuit netlist F_l

1: Perform stuck-at fault injection on F
2: Record set T_f of failing input test patterns
3: Select t_{secure} from T_f that is most frequently encountered during RF transceiver operation
4: Set key equal to the k care bits of t_{secure}
5: Generate F_f by removing redundant logic in F
6: Generate $F_{f'}$ by adding logic into F_f to restore functionality for all failing input test patterns in the set $\{T_f - t_{secure}\}$
7: Generate F_l by adding restore unit and XOR gate into $F_{f'}$

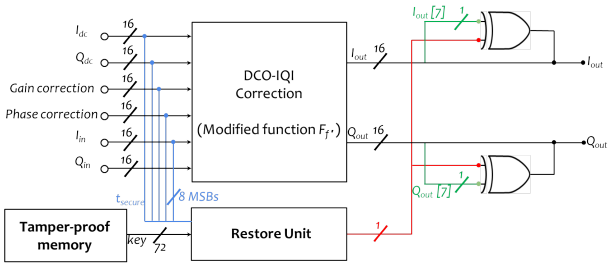

Fig. 2: DCO-IQI correction block with locking mechanism.

correction block and F_l is the DCO-IQI correction block with the lock embedded. The algorithm follows the steps of SFLL-rem detailed in Section III with the third step, i.e., the selection of t_{secure}, being the subject of the tuning. First, in the next paragraph, we explain why tuning is required.

For digital ICs it suffices that logic locking corrupts one bit for a small set of PIPs. For example, to lock a microcontroller it suffices to lock one bit for one input in the program counter to safeguard against unauthorized execution [21]. However, for RF transceiver locking, to ensure an appreciable BER degradation, the transmitted/received data propagated to the input of the DCO-IQI correction block must frequently "hit" one of the PIPs. Thus, t_{secure} that represents the PIPs of the DCO-IQI correction block must be carefully selected specifically to the operation of the RF transceiver.

Let us consider first the DCO-IQI correction block of the receiver. Fig. 2 shows its final high-level block schematic modified by SFLL-rem. The circuit has a 96-bits input, i.e., $n = 96$, and a 32-bit output. We applied SFLL-rem aiming at locking two output bits $I_{out}[7]$ and $Q_{out}[7]$. Let us consider first $I_{out}[7]$. For the logic cone driving $I_{out}[7]$, in the first step of the SFLL-rem procedure, we injected a stuck-at-0 fault that resulted in a large number of failing input test patterns.

To achieve a high security level against all foreseen counter-attacks, as will be discussed in Section V, we need to consider a key of large size k. At the same time, BER degradation requires first ensuring a high error rate expressed as the ratio of PIPs to all input patterns, i.e., $ER = 2^{n-k}/2^n = 2^{-k}$. Increasing k improves resiliency against attacks but reduces the error rate. Furthermore, t_{secure} must be chosen to ensure that the 2^{n-k} PIPs frequently appear, thus resulting in BER degradation. A desired trade-off can be established by choosing appropriately k and t_{secure}.

In this regard, we consider further only those failing input test patterns having $k = 72$ care bits and $n - k = 24$ don't care bits with the don't care bits being the bits of Q_{in}

TABLE I: Subset of failing input test patterns for logic cone driving $I_{out}[7]$ showing only the I_{in} segment.

Pattern	Binary	Signed decimal value range
I	1111 1101 xxxx xxxx	[-640, -513]
II	1111 1110 xxxx xxxx	[-384, -257]
III	1111 1111 xxxx xxxx	[-128, -1]
IV	0000 0000 xxxx xxxx	[128, 255]
V	0000 0001 xxxx xxxx	[384, 511]
VI	0000 0010 xxxx xxxx	[640, 767]

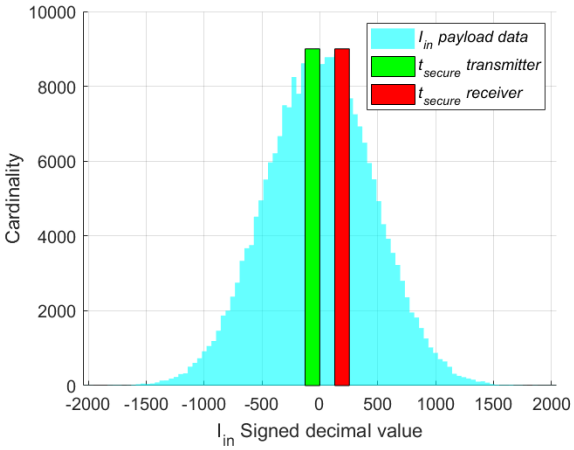

Fig. 3: Histogram of I_{in} payload data during the RF transceiver operation.

and the 8 less significant bits (LSBs) of I_{in}. Table I lists a small subset of the failing input test patterns showing only the I_{in} segment. Among all failing input test patterns, we select t_{secure} to be the one that is most frequently encountered during the RF transceiver operation. To make this selection, we examine the histogram of I_{in} payload data, shown in Fig. 3. The histogram represents I_{in} in signed decimal values and shows their frequency of appearance. Similarly, the segments of I_{in} in Table I are represented with their signed decimal value range resulting from the don't care bits. Now, we can examine where the range of each failing input test pattern lies with respect to the peak of the histogram and select t_{secure} to be a failing input test pattern whose range is close to the peak. The selected t_{secure} is the failing input test pattern IV highlighted in red in Table I, and its corresponding range is also depicted in Fig. 3. The key stored in the TPM is composed of the k=72 care bits of t_{secure}, as shown in Fig. 2.

The next steps in SFLL-rem are to remove logic in the DCO-IQI correction block, resulting in version F_f of the circuit, and then add logic to restore the functionality at the $I_{out}[7]$ output for all failing input test patterns except t_{secure}, resulting in version $F_{f'}$. In the final step, the restore unit and two 2-input XOR gates are added to generate the target circuit F_l that restores functionality at the $I_{out}[7]$ output for t_{secure} when the correct key is applied, as shown in Fig. 2.

The procedure is repeated for the logic cone driving $Q_{out}[7]$ and we force the same t_{secure} to be part of the set of failing input test patterns and selected it. In this way, we have a single t_{secure} and, thereby, a single key locking both logic cones.

The DCO-IQI correction block is the same for the receiver

and the transmitter and the exact same procedure is followed for inserting the locking mechanism into the transmitter as well. However, among all failing input test patterns we selected a different t_{secure}, in particular the failing input test pattern III highlighted in green in Table I and in Fig. 3, such that the receiver and the transmitter have different secret keys.

V. Security analysis

We consider the threat model that is most favorable for an attacker. In particular, we assume that the attacker possesses the transistor-level netlist of the non-activated circuit and an unlocked functional chip which can be used as an oracle.

We observe that any incorrect key results in functionality corruption for the same PIPs. Thus, for a given transmission, the BER degradation is the same for all incorrect keys.

The attacker may try to find the key by iterative simulation searching in the key space in a brute-force fashion or using optimization aiming at maximizing performance, i.e., minimizing BER. For a brute-force attack, the attack time is on average $2^k \cdot T/2$, where T is the run-time of a single simulation. For an optimization attack, the attack time is $m \cdot T$, where m is the number of iterations until convergence is achieved. As T is long for RF transceiver simulation, the attacker can afford running only a limited number of iterations. In this regard, the large key space, i.e., 2^{72} in our implementation, is a strong defense against these attacks. Moreover, since all incorrect keys result in the same degraded BER, the function BER$= g(K)$ relating BER with the key is a delta function and the search cannot be guided with optimization.

The attacker may also attempt to break the defense by performing an attack on logic locking targeting solely the locked DCO-IQI correction block independently of the rest of the RF transceiver blocks. Main attacks are based on input-output query using the netlist and oracle to find the key or structural analysis that exploits the processing by logic synthesis tools to identify and remove the lock mechanism. In this case, the proposed RF transceiver locking strategy inherits the resiliency of the underlying logic locking technique. SFLL-rem offers provable security against input-output query attacks [4], but recently has shown vulnerability to a structural attack and a mitigation solution is proposed [22].

VI. Experimental Results

A. Hardware Platform

We use the SDR bladeRF board from Nuand™. This board contains three main chips: an Analog Front-End (AFE) LMS6002 from Lime Microsystems™, a Field-Programmable Gate Array (FPGA) Cyclone IV from ALTERA™, and a USB 3.0 peripheral controller FX3 from Cypress™. The RF transceiver has a conventional Zero-IF architecture for both the receiver and the transmitter, shown in Fig. 1a. The DCO-IQI correction blocks are programmed inside the FPGA. The AFE has an on-chip loopback mode allowing us to perform BER measurements using the same board. This also greatly simplifies the channel model, allowing us to assume an Additive White Gaussian Noise (AWGN) channel model.

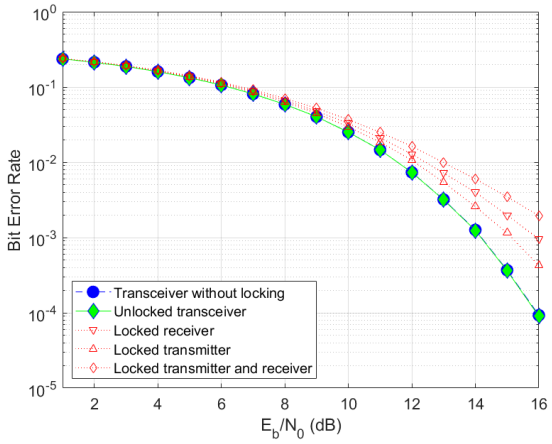

Fig. 4: BER measurement results for different configurations.

We implemented a wireless telecommunication protocol using for the payload an Orthogonal Frequency Division Multiplexing (OFDM) encoding with a 16 Quadrature Amplitude Modulation (16-QAM) scheme in each carrier, and the SDR is transmitting and receiving in the Industrial, Scientific and Medical (ISM) unlicensed band at 2.4 GHz.

As metric of performance, we consider the BER versus the energy per bit, E_b, to noise power spectral density ratio, N_0, i.e., E_b/N_0. We also present received constellation diagrams.

B. Measured locking efficiency

Fig. 4 shows the measured BER versus E_b/N_0 for five scenarios. The first scenario is the nominal design with no locking mechanism, while the other four scenarios correspond to the design with the locking mechanism embedded, where "unlocked" means that the correct key is applied and "locked" means that an incorrect key is used. As explained in Section V, considering a given locking scenario with an incorrect key, the measured BER curve is exactly the same regardless which incorrect key is used. For this reason, in Fig. 4, we use the term "locked" to refer to applying an incorrect key in general.

The following observations can be made from Fig. 4:

1) Embedding the locking mechanisms into the DCO-IQI correction blocks has zero performance penalty since the BER curves of the RF transceiver without locking mechanism and the unlocked RF transceiver are identical.

2) Using an incorrect key for the receiver, transmitter or both, degrades BER and the degradation worsens with E_b/N_0. By locking both the receiver and the transmitter, BER is degraded by more than one order of magnitude for E_b/N_0 higher than 15dB. Note that the goal is to achieve enough BER degradation to the point where the RF transceiver is deemed of unacceptable quality.

3) BER degradation is higher when locking only the receiver compared to locking only the transmitter. The reason is that the PIPs of the DCO-IQI correction block of the receiver are more frequently encountered in the communication compared to those of the DCO-IQI correction block of the transmitter. BER degradation is higher when both the receiver and transmitter are locked since now the set of PIPs becomes the union of the

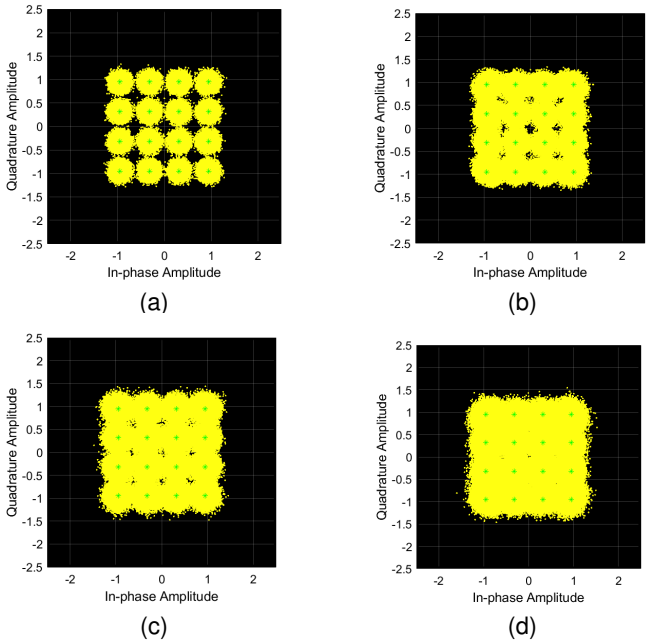

Fig. 5: Measured I/Q constellation diagrams. (a) Unlocked transceiver. (b) Locked receiver. (c) Locked transmitter. (d) Locked receiver and transmitter.

PIPs of the DCO-IQI correction blocks of the receiver and the transmitter.

Fig. 5 shows the measured I/Q constellation diagram of the received signals for the last four scenarios. Locking causes constellation points to clearly deviate from their ideal locations compared to the unlocked transceiver.

C. Locking Overheads

Due to the locking operation, the area, power consumption, and delay of the DCO-IQI correction block are increased by 3.9%, 0.3%, and 0.8%, respectively. As it can be seen from Fig. 4, there is no BER performance penalty implying that the small delay penalty is fully absorbed. Moreover, considering a fully integrated implementation of the RF transceiver, the DCO-IQI correction block is a small block, thus these small area and power overheads become negligible when projected to the entire RF transceiver. Therefore, we can claim a near zero area and power overhead due to locking.

VII. Conclusions

We demonstrated for the first time RF transceiver locking against piracy. The methodology is based on logic locking of digital blocks in the signal processing chain. We employed the state-of-the-art SFLL-rem logic locking technique and we adapted it for effective RF transceiver locking. The methodology is virtually applicable to any RF transceiver architecture and inherits the security properties of logic locking. Hardware experiments demonstrated strong BER degradation for incorrect keys, while achieving zero performance penalty when applying the single correct secret key, and negligible area and power overheads. The methodology can be seamlessly integrated into the RF transceiver design flow since its analog section is left intact and logic locking is fully automated.

References

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[2] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending piracy of integrated circuits," *Computer*, vol. 43, no. 10, pp. 30–38, Oct. 2010.

[3] A. Chakraborty *et al.*, "Keynote: A disquisition on logic locking," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 1952–1972, Oct. 2020.

[4] A. Sengupta, M. Nabeel, N. Limaye, M. Ashraf, and O. Sinanoglu, "Truly stripping functionality for logic locking: A fault-based perspective," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4439–4452, Jan. 2020.

[5] J. Leonhard *et al.*, "MixLock: Securing mixed-signal circuits via logic locking," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, p. 84–89.

[6] J. Leonhard *et al.*, "Digitally-assisted mixed-signal circuit security," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, 2021, early access.

[7] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, "Towards provably-secure analog and mixed-signal locking against overproduction," in *Proc. 18th Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2018.

[8] D. H. K. Hoe, J. Rajendran, and R. Karri, "Towards secure analog designs: A secure sense amplifier using memristors," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, Jul. 2014, pp. 516–521.

[9] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sánchez-Sinencio, and J. Hu, "Thwarting analog IC piracy via combinational locking," in *Proc. IEEE Int. Test Conf. (ITC)*, Oct. 2017.

[10] G. Volanis, Y. Lu, S. Govinda, R. Nimmalapudi, A. Antonopoulos, A. Marshall, and Y. Makris, "Analog performance locking through neural network-based biasing," in *Proc. IEEE VLSI Test Symp. (VTS)*, Apr. 2019.

[11] V. Rao and I. Savidis, "Performance and security analysis of parameter-obfuscated analog circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 12, pp. 2013–2026, Dec. 2021.

[12] S. G. Rao Nimmalapudi, G. Volanis, Y. Lu, A. Antonopoulos, A. Marshall, and Y. Makris, "Range-controlled floating-gate transistors: A unified solution for unlocking and calibrating analog ICs," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar 2020.

[13] M. Elshamy, A. Sayed, M.-M. Louërat, A. Rhouni, H. Aboushady, and H.-G. Stratigopoulos, "Securing programmable analog ICs against piracy," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2020, pp. 61–66.

[14] M. Tlili, A. Sayed, D. Mahmoud, M.-M. Louërat, H. Aboushady, and H.-G. Stratigopoulos, "Anti-piracy of analog and mixed-signal circuits in FD-SOI," in *Proc. 27th Asia South–Pac. Design Autom. Conf. (ASP-DAC)*, Jan. 2022, pp. 423–428.

[15] N. G. Jayasankaran, A. Sanabria-Borbón, A. Abuellil, E. Sánchez-Sinencio, J. Hu, and J. Rajendran, "Breaking analog locking techniques," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, Oct. 2020.

[16] V. V. Rao, K. Juretus, and I. Savidis, "Security vulnerabilities of obfuscated analog circuits," in *Proc. IEEE Int. Symp. Circuits and Syst. (ISCAS)*, Oct. 2020.

[17] R. Y. Acharya, S. Chowdhury, F. Ganji, and D. Forte, "Attack of the genes: Finding keys and parameters of locked analog ICs using genetic algorithm," in *Proc. IEEE Int. Symp.Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 284–294.

[18] J. Leonhard, M. Elshamy, M.-M. Louërat, and H.-G. Stratigopoulos, "Breaking analog biasing locking techniques via re-synthesis," in *Proc. 26th Asia South Pacific Design Automat. Conf.*, Jan. 2021, p. 555–560.

[19] A. Sanabria-Borbón, N. G. Jayasankaran, J. Hu, J. Rajendran, and E. Sánchez-Sinencio, "Analog/RF IP protection: Attack models, defense techniques, and challenges," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 36–41, Jan. 2021.

[20] A. Sayed, T. Badran, M. Louërat, and H. Aboushady, "A 1.5-to-3.0GHz tunable RF sigma-delta ADC with a fixed set of coefficients and a programmable loop delay," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 9, pp. 1559–1563, Sep. 2020.

[21] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. Rajendran, and O. Sinanoglu, "Provably-secure logic locking: From theory to practice," in *Proc. ACM SIGSAC Conf. Comput. and Commun. Security*, Oct. 2017, pp. 1601–1618.

[22] Z. Han, M. Yasin, and J. Rajendran, "Does logic locking work with EDA tools?," in *Proc. 30th USENIX Security Symposium*, Aug. 2021.