Active IC metering of digital signal processing subsystem with two-tier activation for secure split test

Dhabu, Sumedh Somnath; Zheng, Yue; Liu, Wenye; Chang, Chip Hong

2018

Dhabu, S. S., Zheng, Y., Liu, W., & Chang, C. H. (2018). Active IC metering of digital signal processing subsystem with two-tier activation for secure split test. 2018 IEEE International Symposium on Circuits and Systems (ISCAS). doi:10.1109/ISCAS.2018.8351390

https://hdl.handle.net/10356/80470

https://doi.org/10.1109/ISCAS.2018.8351390

Active IC Metering of Digital Signal Processing Subsystem with Two-Tier Activation for Secure Split Test

Sumedh Somnath Dhabu, Yue Zheng, Wenye Liu, and Chip-Hong Chang
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore

***Abstract*—Active integrated ciruit (IC) metering is a class of hardware security protocols that enables the designer to track the number of chips produced from the same mask and remotely activate only the desired ones. This paper reviews existing IC metering approaches to incorporate the advantages of individual methods into a secure functional lock on digital signal processing submodule of wireless communication to avoid legitimate channel exploitation and the risk of deploying unreliable out-of-specs gray market ICs. Our method makes use of aging-sensitive physical unclonable function to enable a two-tier activation of ICs in split test flow to track chip supply after production tests. Extraneous states are inserted into the state-space mapping of digital signal processing submodule as opposed to controller to provide a stronger state dependent on datapath and input signal. The scheme is illustrated experimentally on a pulse shaping filter of the transmitter for a wireless communication system.**

I. Introduction

The cost of building, operating and upgrading a semiconductor fabrication plant and its clean room facilities is escalating with the rapid renewal of technology. Economic of scale driven by equipment utilization rate and production capacity has led to the paradigm separation of design and manufacturing into fabless semiconductor companies and merchant foundries. The latter includes pure-play foundries that only manufacture products contracted by other companies and integrated device manufacturers who also fabricate their own designed products with no conflict of interest to their clients products. This horizontal foundry model has threatened the trustworthiness of integrated circuit (IC) supply chain. One major concern is the unfair predicament of design transparency. The designer provides all the necessary details of their design to the merchant foundry in the form of layout and netlist for mask creation and chip fabrication. Once a mask is built, the designer has to trust the foundry to fabricate, test, and provide the contracted number of structurally and functionally correct in-spec chips. The foundry, on the other hand, has full control over the production volume, fabrication process and testing parameters. This gives an untrusted foundry to outright exploit and manipulate the physical design to their advantage. An untrusted foundry may reuse the same mask to fabricate additional ICs, label the defective ICs as in-spec ICs, and sell them for profit in the gray market, or collude with other clients to reverse engineering or pirating the intellectual property (IP).

In order to provide the designer with a fair control over the fabricated ICs, a new class of hardware security protocols has emerged and received considerable attention recently. These IC metering techniques enable the designer to monitor the number of ICs produced with the same mask by disabling the core functionality of the design prior to manufacturing and/or remotely enable/disable the circuit upon manufacturing to facilitate chip testing, field deployment and system integration. The emergence of lightweight physical unclonable function (PUF) has further augmented such a scheme by providing a device-specific unique identifier to track each chip fabricated from an identical physical design without having to hard code or store the device ID which can be easily reverse engineered from the layout. A PUF explicitly utilizes the physical disorder of the random process variations of nanoscale fabrication facilities of semiconductor devices to produce a unique and unpredictable digital bitstream upon stimulation. This makes it possible to design a locking mechanism that is identical for all chips but each locked chip that carries the same design can only be activated and deactivated by a unique key derived from the response of the PUF. The core advantage of using PUF to identify the chip in active metering scheme is that the physical disorder is prohibitively difficult to replicate precisely with existing fabrication technology, even if its entire structure is known by the manufacturer.

In this paper we review the active metering schemes, discuss their limitations and propose a subtle modification to aptly apply active IC metering scheme on digital signal processing (DSP) subsystem of a communicaton chip. Our scheme enjoys the advantages of computationally intractable recovery of the FSM obtained from state-space model of a DSP circuit and two-tier activation with aging-sensitive PUF and split test strategy to provide the designer with a complete control over the testing of fabricated chips and chips shipped after production tests. In contrast to embedding the locking mechanism directly into the control circuitry of an IC, the state-space mapping of selected DSP subcircuit provide a tight coupling with the datapath and input signal, making attempt to replace control logic to manipulate the added non-functional states more difficult to succeed. In Section II we discuss the state-of-the-art IC metering methods that motivates their enhanced application on signal processing modules. In Section III, we present the proposed scheme. The experiment results are discussed in Section IV. Section V concludes this paper.

II. A Scrutiny of State-of-the-art IC Metering Method

One main approach to provide production control is to modify the control logic of an IC, which is typically specified and designed as an FSM, to prevent the access to its circuit

functionality [1], [2]. The FSM is modified in such a way that its initial state is brought to one of the added non-functional states by the embedded PUFs response to a default challenge. The locked FSM can only be correctly reset by a specific bit sequence to be input by the user. The length of the key to unlock the FSM should be sufficiently long to prevent brute-force attack by making the probability of correct wild guess extremely low. Due to the uniqueness of PUF response, each IC is locked in a different non-functional state. The key to unlock the FSM can only be generated by the designer who has the knowledge of the complete state transitions of the modified FSM design. Based on the response of the embedded PUF measured by the foundry for each chip, the designer can determine the locked non-functional state and derive the key to activate the locked IC by bringing it out of the non-functional state. This IC-specific key is then programmed into its non-volatile memory (NVM) so that the IC can reset normally for testing thereafter. This way the designer is able to track the number of ICs produced by the foundry as overproduced chips are useless without a valid key provided by the designer to activate these chips. The main limitation of such approach is that once the IC is unlocked for post-production testing, the designer has no control over it. The foundry can overproduce the ICs, request for their corresponding keys by claiming low yield or lower number of in-spec ICs, and then return only the contracted number of ICs to the designer [3].

To address the above limitation, a secure split test flow was proposed in [4], [5]. In split testing, the foundry sends back the structural test results of a locked chip to the designer (who is the only person that can interpret the test results of a specific locked chip) for verification, along with the unique identification number of each IC (generated by, for example, its embedded PUF response). Only if the IC passes the tests will the designer provide the untrusted foundry its activation key to unlock the IC. As the functional tests have to be carried out on an unlocked IC [3], the foundry can still claim lower (than actual) passing rate after the functional tests and request for the activation keys on overproduced ICs in order to meet the volume of sale. The foundry may then sell the extra in-spec ICs or out-of-spec ICs as in-spec ICs in the gray market.

The abovementioned deficiency is elegantly circumvented by an input, output and logic obfuscation with an aging-sensitive PUF for secure split test method in [3]. The scheme makes use of temporary and permanent internal and external keys for de-obfuscating the IO and design logic in chip testing and deployment phases. The PUF response determines the internal key, whereas the external key is provided by the designer based on the knowledge of the obfuscation logic and the internal key. A temporary fingerprint generated by the embedded PUF response after chip manufacturing is sent to the designer to derive an external key. Meantime, the temporary fingerprint is also fed to an internal linear feedback shift register (LFSR) to generate a temporary internal key for chip testing. An on-chip parser converts the temporary fingerprint to a permanent fingerprint which is stored in an on-chip NVM. During chip testing phase, the foundry uses the external key supplied by designer to unlock the IC, conducts the structural and functional tests and sends the results back to the designer for verification. For confidentiality, these results are encoded using an on-chip convolutional compactor seeded by the internal key. The aging-sensitive PUF in [3] ensures that the PUF response is valid only for 2-3 months, which is a sufficient time window for the testing phase. Once the PUF response expires, the previous external key becomes invalidated. To prolong the usage of the chip, a new internal key has to be generated from the permanent fingerprint for chip activation. From the knowledge of the structures of parser and temporary fingerprint, the designer can supply the new device-specific external keys only for those ICs which are shown to be in-spec by the logged results. This combination of split test flow and aging-sensitive PUF ensures that chip usage after the production test requires a fresh activation, hence providing the designer a control over the number of in-spec ICs being released in the market.

As the LFSR used to convert the external fingerprint to internal key and the parser used to convert the temporary fingerprint to permanent fingerprint are common to all the ICs, the security of the scheme [3] relies on the secrecy of these two structures. In order to protect these structures against reverse engineering attacks, a camouflaged layout [6] is suggested in [3]. Camouflaged layout can still be reverse engineered within a very short time span with only moderate computing power according to [7]. An attacker who has access to temporary fingerprint and external key of only one IC, and has the de-camouflaged LFSR and parser structures, can defeat this protection scheme as follows. The attacker first computes the internal key for that IC. Based on the internal and external keys, the attacker can work out the obfuscation logic inserted by the designer, which is a straightforward task when both the keys are known. Then, using the knowledge of parser structure, the attacker can calculate the permanent fingerprint for any IC from its temporary fingerprint to gain access to the internal key of that IC. As the obfuscation logic is common to all the ICs, calculating the external key is also a trivial task. An attacker, such as a foundry, can overbuild and sell the ICs without having to spend significant amount of time and resources on removing or modifying the obfuscation logic, which is actually a more computationally expensive task. Therefore, despite the fortification of split test by using aging-sensitive PUF and data logger for testing phase results, the security of this method [7] as a whole may suffer from this weak link.

III. Proposed Enhancements to IC Metering

Compared to using LFSR camouflage and common parser structure with obfuscation logic, FSM is more resilient against reverse engineering attack as recovery of its state transition graph (STG) is a computationally intractable problem for a sufficiently complex FSM [1]. The locking mechanism of existing FSM based active metering methods is usually embedded in the control circuitry of the design. This may create the potential vulnerability of successful erasure or replacement of the control logic. It turns out that mapping a domain-specific signal processing module directly into FSM provides a tight coupling between the datapath and extraneous states inserted into the design. To overcome the inability to track overproduced and out-of-spec ICs after unlocking their FSMs for production test, time-bound PUF response and split test

flow are adopted. The external key used to unlock the IC for the purpose of manufacturing testing is made to expire after a qualification period controlled by a carefully designed aging circuit. Thereafter a new external key is required to activate the IC permanently. Without loss of generality, such a secure locking mechanism is embedded into the transmitter circuit of a wireless communication system for demonstration, where some part of the cascaded filter chain is converted into FSM.

Finite impulse response (FIR) filters are widely used in transmitters and receivers for spectrum sensing, spectrum shaping, digital up/down-conversion, channel error correction etc. For a typical wireless communication system, usually the standard is defined by broad specifications in terms of minimum and/or maximum limits on throughput rate, latency, bit-error-rate, spectral mask, adjacent channel interference, intermediate frequency, etc. The specific design and implementation details such as the number of stages in filter chain, exact frequency response, filter coefficients, filter structure, quantization parameters of each filter, etc. are left to the designers preference, as long as the desired specifications of the standard are met. The choice of such details decides the quality of the design and area/power efficiency, which are important design assets particular in multi-standard communication systems. Protection of these design modules is not merely a concern of IP piracy but also of legitimate channel exploitations to disguise prohibitive information.

The signal processing module of a wireless communication system can be represented by an FSM. For the purpose of illustration, we consider the state-space mapping of a 3-tap FIR filter with an 1-bit input and a 3-bit output as shown in Fig. 1. The filter coefficients $\{1, 2, 1\}$ are each represented by a 2-bit word. For every input, the state of this filter is uniquely defined by the values at P1, P2 and P3, where P3 is also the output. The corresponding STG with 8 states is shown in Fig. 2. Each state is annotated by the corresponding values at P1, P2 and P3 below its mnemonic. The processing results of the datapath and input signal have now a direct correspondence on the states and influence on the state transitions of the FSM.

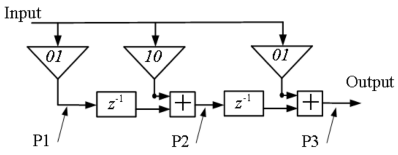

Fig. 1. A 3-tap FIR filter.

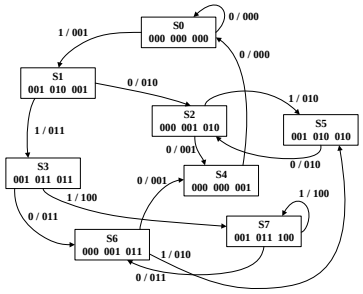

Fig. 2. STG Transformation of FIR filter in Fig. 1.

The locking mechanism involves a PUF whose response to a fixed challenge is mixed with an aging indicator signal a_i. This aging-sensitive PUF response determines the initial state after power-up reset. It also controls the transition of the FSM. Using a 15-bit PUF response for illustration, seven bits of the original PUF response (e.g., PUF[6:0]) will be selectively XORed with ai to generate a Path1 selector signal, while the remaining eight bits of original PUF response will be XORed with the external key K_e to generate the Path2 selector signal. As shown in Fig. 4, a layer of non-functional states rep1 to rep128 are added before the functional reset state s0. The FSM will be reset to the non-functional state rep0 before it is triggered into one of the 128 nonfunctional replicated states by Path1 selector. To produce the correct filters output, a correct input is required to move the signal out from the non-functional state to s0. This input is provided by entering the correct K_e into the Path2 selector. To generate the correct external key K_e, the designers knowledge of the FSM mapping from the FIR filter (or other signal processing module) is required. A wrong K_e will cause the STG to lock in a black hole state that can only transit among the non-functional states irrespective of the inputs.

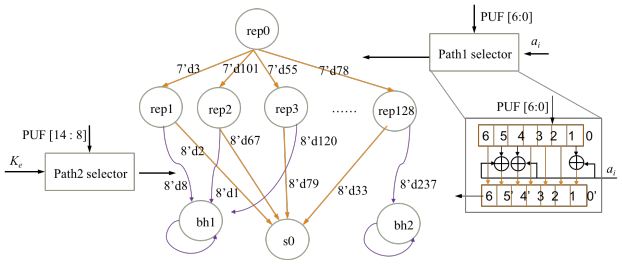

Fig. 4. A single-layer PUF-based locking structure.

The connections in Path1 and Path2 are randomly encoded, PUF response bits are also randomly allocated to the Path1 and Path2 selectors, and random connections are used for XOR between PUF response bits used in Path1 selector and a_i. When a_i switch from its original temporary logic state to a permanent logic state after a controlled aging period, Path1 connection will be altered and a different replicated state will be entered upon reset. K_e has to be renewed to permanently activate the filter. This fundamental model can be enhanced by cascaded locks in a hierarchical FSM with longer PUF response and external key as shown in Fig. 5, where the merged functional states are super states. Super states in hierarchical FSM eliminates redundant transition logic, making it harder to identify the connections between functional states within the super state and non-functional states.

IV. Simulation and Implementation Results

In general, the number of states in the corresponding FSM of a FIR filter is a function of possible inputs, number and values of filter coefficients and quantization parameters (bitwidths and quantization method for representing coefficient values, multiplication and addition results). Therefore, the size of FSM increases exponentially with the increase in these parameter values. For our experiment, we judiciously

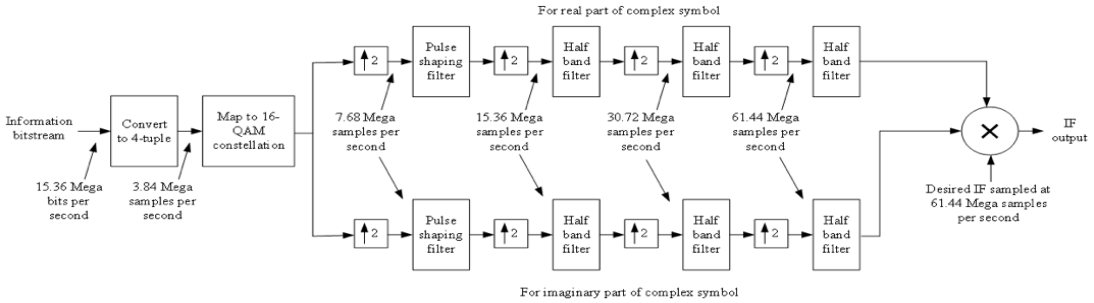

Fig. 3. Transmitter model considered in Section IV.

TABLE I
IMPLEMENTATION RESULTS.

	Reference model	Model A	Model A + single-layer lock, 8-bit K_e	Model A + five-layer lock, 40-bit K_e
Slice (Available 13300)	2681	2667 (-0.52%)	2889 (+7.76%)	3176 (+18.46%)
Power (W)	0.173	0.175 (+1.16%)	0.175 (+1.16%)	0.175 (+1.16%)

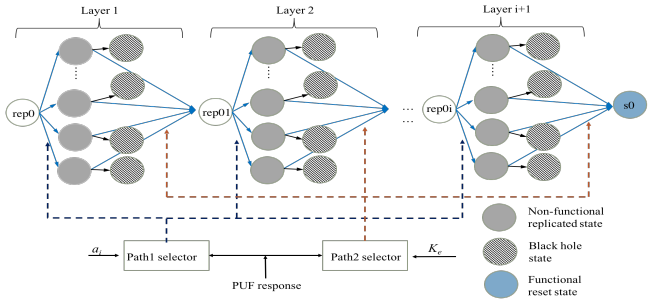

Fig. 5. A multi-layer locking structure.

choose the pulse shaping filter in the filter chain to create a functional lock of the transmitter chain. The transmitter shown in Fig. 3 of a wireless communication system with 16-QAM modulation scheme is used as an example. The sub-blocks of the transmitter are designed with fixed-point arithmetic to meet the spectral mask and frequency specifications of the WCDMA standard. The straightforward implementation of this model is considered as a reference model. The first 3 taps of the pulse shaping filter in the upper chain of filters corresponding to processing of real part of the complex modulated signals is converted to a FSM, the inputs being $\{-3, -1, 1, 3\}$ for real part of 16-QAM symbol and 0 for resetting the filter. Bitwidths and quantization method for fixed-point arithmetic are incorporated in the state-space mapping. The hybrid RO PUF proposed in [8] and the aging indicator signal generator of [3] were implemented for experiments on Xilinx Zedboard xc7z020 FPGA. The transmitter with and without the locked FSM of the first 3-taps showed identical functionality as the reference design, when the correct keys are used for the locked FSM.

Table I shows the number of slices and estimated power consumption reported by the Xilinx Vivado tool after placement and routing for four designs, viz., reference model, FSM without lock (model A) of three filter taps, Model A with single layer lock and Model A with multi-layer lock. Percentage hardware resource and power overheads with respect to the Reference Model are indicated in brackets. The area overhead for Model A with five-layer lock is around 18.5% for this relatively plain transmitter model. A practical transceiver IC will consist of additional blocks, e.g., error correction mechanism, digital IF generator, receiver etc., which will reduce the area overhead significantly.

Two main attacks, viz. reverse engineering attack and the brute force attack, are also analyzed. In the proposed 5-layer locking mechanism, the PUF response size is set to be 75 bits while a 40-bit K_e is required to unlock the IC. The FSM for this example has a total of 770 states and thousands of transitions. The resilience against physical attack of the proposed scheme relies on the computational complexity in extracting the STG of big FSM, which is more difficult than reverse engineering a common paser structure and decamflouging a 64-bit LFSR in [3].

An attacker may also conduct a brute force attack to guess the external key by trying all the possible combinations. The data output rate of the filter is 61.44M. Our simulation result shows that it takes about 20.448 μs for the filter chain to get the steady output. Then in a 5-layer locking mechanism with 40-bit external key K_e, guessing a correct key by trying all the possible combinations requires around 260 days. The time required to conduct brute force attack increases exponentially with the key size. It is found that increasing the key size will gently increase the slice overhead but has a much smaller influence on its power overhead.

V. CONCLUSION

Our review of the state-of-the-art IC metering methods discovered some potential weaknesses, even though the individual concepts used in these methods are elegant and practical. Our observations suggest that IC metering incorporating a two-tier activation in split test can be more advantageously incorporated into the DSP modules, especially for wireless communication, to gain control in chip deployment after test. The extraneous and backhole states inserted after the state-space mapping of DSP submodule and the complexity in reverse engineering large FSM have, to a great extent, eliminated the potential weak links of existing methods.

REFERENCES

[1] F. Koushanfar, "Provably secure active ic metering techniques for piracy avoidance and digital rights management," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 51–63, Feb. 2012.

[2] Y. Alkabani, F. Koushanfar, and M. Potkonjak, "Remote activation of ICs for piracy prevention and digital right management," in *Proc. 2007 IEEE/ACM Int. Conf. Computer-Aided Design*, San Jose, CA, Nov 2007, pp. 674–677.

[3] X. Wang, Y. Guo, M. T. Ramhan, D. Zhang, and M. Tehranipoor, "DOST: Dynamically obfuscated wrapper for split test against IC piracy," in *Proc. 2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, Beijing, Oct. 2017.

[4] G. K. Contreras, M. T. Rahman, and M. Tehranipoor, "Secure split-test for preventing IC piracy by untrusted foundry and assembly," in *Proc. 2013 IEEE Int. Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, New York, US, Oct 2013, pp. 196–203.

[5] M. T. Rahman, D. Forte, Q. Shi, G. K. Contreras, and M. Tehranipoor, "CSST: Preventing distribution of unlicensed and rejected ICs by untrusted foundry and assembly," in *Proc. 2014 IEEE Int. Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*, Amsterdam, Oct 2014, pp. 46–51.

[6] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security analysis of integrated circuit camouflaging," in *Proc. ACM Sigsac Conf. Computer Communications Security*, Berlin, Germany, Nov. 2013, pp. 709–720.

[7] M. E. Massad, S. Garg, and M. V. Tripunitara, "Integrated circuit (IC) decamouflaging: Reverse engineering camouflaged ICs within minutes," *Network and Distributed System Security Symposium*, Feb. 2015.

[8] Y. Cao, L. Zhang, C. H. Chang, and S. Chen, "A low-power hybrid RO PUF with improved thermal stability for lightweight applications," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 7, pp. 1143–1147, July 2015.