A Novel PUF based SST to Prevent Distribution of Rejected ICs from Untrusted Assembly

Sudeendra kumar K, Hanumanta Rao G, Sauvagya Sahoo, K.K.Mahapatra
kumar.sudeendra@gmail.com
National Institute of Technology, Rourkela.

***Abstract*- Globalization of semiconductor design, manufacturing, packaging and testing has led to several security issues like over production of chips, shipping of faulty or partially functional chips, intellectual property infringement, cloning, counterfeit chips and insertion of hardware trojans in design house or at foundry etc. Adversaries will extract chips from obsolete PCB's and release used parts as new chips into the supply chain. The faulty chips or partially functioning chips can enter supply chain from untrusted Assembly Packaging and Test (APT) centers. These counterfeit parts are not reliable and cause catastrophic consequences in critical applications. To mitigate the counterfeits entering supply chain, to protect the Intellectual Property (IP) rights of owners and to meter the chip, Secure Split Test (SST) is a promising solution. CSST (Connecticut SST) is an improvement to SST, which simplifies the communication required between ATP center and design house. CSST addresses the scan tests, but it does not address the functional testing of chips. The functional testing of chips during production testing is critical in weeding out faulty chips in recent times. In this paper, we present a method called PUF-SST (Physical Unclonable Function –SST) to perform both scan tests and functional tests without compromising on security features described in CSST.**

Keywords: **Counterfeiting, secure split test, hardware metering.**

I. INTRODUCTION

The common security problems known in semiconductor industry are counterfeit chips, IP protection, hardware trojans, side channel analysis of cryptographic engines, and debug security against reverse engineering schemes [1]. In this paper, we focus mainly on counterfeit electronics. Counterfeit electronic devices are becoming a significant threat to industry, government and defense systems. The counterfeit electronics used in critical systems like aerospace, automotive and defense systems challenge the reliability and security of those systems. And counterfeits damage the reputation of semiconductor suppliers and lead to unwanted litigations leading to financial losses. In most of the cases, the original company will replace the failed counterfeit parts and pay huge fines. E-waste generated out of obsolete electronic products is extremely huge and counterfeiters will break the PCB boards and extract the components [2]. Counterfeiters polish the extracted components and sell in the open market. E-waste is major resource for counterfeit components. Another source of counterfeit electronic components is untrusted contract manufacturing factories and Assembly-Packaging-Test (APT) centers. Due to globalization of the semiconductor supply chain, chip makers fragmented their different operations to different geographies to reduce the cost and to stay competitive in the market. These untrusted factories may overproduce the chips without approval of the original component company and sell in open markets. In the similar way, untrusted APT centre may sell failed and out of specification chips. According to professional ethics, contract manufacturers should not overproduce the chips, without approval of original component manufacturer and ATP centre must destroy or send the failed chips back to original device manufacturer. The untrusted foundries and ATP centers can become a source for counterfeit parts [3] [4].US Bureau of Industry and Security Office of Technology Evaluation studied how counterfeit electronics infiltration into weapon systems affects the reliability. Major semiconductor suppliers to US defense participated in the study and found counterfeit versions of their products. Counterfeit electronics market is growing at a large scale which is a threat to reliability of defense systems, automotives and medical equipment. It is a challenging task for engineers and researchers to find suitable techniques to mitigate the counterfeit parts entering the supply chain [5] [6].

Hardware metering is one promising technique to check the overproduction of chips in untrusted foundries. Active hardware metering using physical unclonable functions (PUF) is an attractive solution to counter over production of chips. This PUF based active metering also finds an application in IP protection [8] [9] [10]. The secure split test (SST) technique was proposed in [11] to mitigate the infiltration of failed or out of specification chips into supply chain from APT centres. An improvement or simplified approach for SST called Connecticut SST (CSST) was proposed by same researchers in [12] [13].

This work is an improvement to the CSST proposed in [13]. In CSST, chips are tested for manufacturing faults and functional key for good chips is generated and programmed into the one time programmable memory (OTP). In recent times, there is a need to incorporate functional tests in production testing of integrated circuits. The modern day System on chip testing demands inclusion of few critical functional tests during final production test [29, 30]. CSST architecture support structural tests and does not address functional testing. In this work, we propose a novel SST architecture which includes both structural and functional tests during final production test. The section II discusses the CSST in detail. Section III will give overview of Physical unclonable function and discusses the choosing a suitable PUF for SST. Section IV presents the proposed architecture and results are discussed in section V. Finally section VI concludes the paper.

II. PRELIMINARIES

In this section we discuss two security techniques against counterfeiting: Hardware metering and SST. Hardware Metering or IC metering is a process of enabling the design house to implement post fabrication controls on IC. The term hardware metering is coined in 2001 in [9] [15]. The purpose of hardware metering is device identification and authentication. Extended versions of active metering are used in Intellectual Property (IP) protection and digital rights management [16]. In recent years, physical unclonable function (PUF) based hardware metering is proposed in [8] [9-10]. The passive metering techniques like storing the device ID in non-volatile memory for identification is followed by major

semiconductor manufacturers. Active metering based on PUFs is more resistant to counterfeiting attacks [10].

The active and passive hardware metering techniques discussed above address the counterfeiting problem arising from untrusted foundry. The hardware metering will not address the out of specification parts or failed parts from untrusted APT centres may enter supply chain. SST is a technique proposed in [11] to address this issue. The improved version of SST is CSST proposed in [12-13]. CSST is a technique to stop the failed devices from APT centres entering supply chain and has got a feature of functional locking useful for active metering or IP protection. The block diagram of CSST is shown in figure 1.

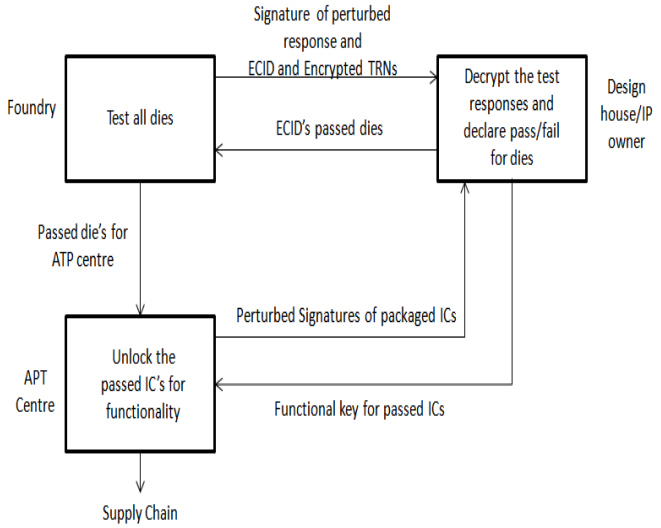

Figure 1: CSST communication between foundry, APT centre and design house [13]

The main feature of CSST is establishing the secure communication between the design house and foundry/APT centre. The block diagram of CSST presented in [13] is shown in figure 2.

- ✓ CSST structure consists of True Random Number Generator (TRNG) to generate random number and RSA block to encrypt the random number. The part of the random number is used in scan locking and another part will be used for functional locking. The random numbers generated will be unique for a given device. The random number is used to scramble the output of scan chains so that, the true responses of the device is unknown (pass/fail) to foundry/APT centre.
- ✓ The outputs of scan chains are scrambled. Random number generated by TRNG is used to scramble the scan chain output, so that in each device scrambling logic is different.
- ✓ The TRNG is used only once and the random number generated is stored in one time programmable (OTP) memory.
- ✓ On-chip RSA is used for encryption of random numbers of each die using public key at foundry/APT centre.
- ✓ Foundry applies test patterns to each die and collects encrypted random number, scrambled test signature and chip id and send it to design house.
- ✓ Design house determines which die in the wafer has passed/failed in testing by decrypting the random number, scrambled test responses and chip id using the private key of RSA. Design house segregate the passed/failed die chip id's by comparing the test signature response of each die with golden signature. Then design house will communicate the list of fault free chip id's with foundry. Foundry will mark the failed dies on wafers on ship it to APT centres.
- ✓ Wafers will be diced, packaged and tested at APT centres. Design house will send part of the random number to the APT centre, represented as R_{IP} in [13]. This new random number sent to APT centre will be used to scramble the scan outputs in a different way than wafer sorting. So APT can't send packed dies back to designer without testing.
- ✓ The APT centre will send the chip id, scrambled test signature to design house to decide on the test result for each IC.
- ✓ Design house will send the different functional key for each chip to unlock the design functionality. No functional key is generated for failed ICs and they remain unlocked functionally. It is easy to identify failed chips in the supply chain, if they get inserted.

The CSST is a better technique than earlier active hardware metering techniques. CSST addresses the counterfeiting in the supply chain more holistically. It involves foundry, APT centre and design house with secure communication link which is vital for fabless original component manufacturer.

There are three papers on secure split test. The paper [11] introduces the concept of SST, the second paper [12] simplifies the communication between foundry and design house and finally third paper [13] completes the SST by integrating APT centre. SST is more efficient technique than other counterfeiting methods like active hardware metering etc. The analysis of possible attacks on SST is also discussed in earlier papers. The SST presented in all three papers has got following disadvantage:

- ✓ The most of the test patterns run during final production test are structural tests. In recent times, inclusion of few crucial functional tests in production test run is required to weed out faulty chips. In the present SST technique it is not clear how XOR gates associated with functional locking of chip work when functional test is performed. The SST proposed in [11] [12] [13] is to perform structural tests and does not support functional testing. During testing phase, no functional key is generated and key is required to unlock the XOR gates associated with functionality of chip. So functional testing is not possible in present CSST design.
- ✓ The functional locking scheme is weak and only using layer of XOR gates are used to lock the design is not sufficient [13].

To address the above disadvantages, we propose a novel PUF based SST technique.

III. PHYSICAL UNCLONABLE FUNCTION

Physical unclonable functions (PUFs) are a promising security primitive used for authentication and cryptographic key storage. The storing secret keys in memories are vulnerable to attacks. PUFs derive a secret key from the process variation that occurs during fabrication of integrated circuit. There is no need to change mask and manufacturing process during fabrication. PUF circuits leverage the process variations which occur in manufacturing of chip. PUF circuit in each chip will have its own unique characteristics derived from manufacturing variability [10]. It is highly difficult to manufacture another identical chip with same PUF circuit characteristics even with full knowledge of the chip. PUF circuits exploit the multiple variations occur during manufacturing like gate delay, interconnect delay, threshold voltages etc to get the uniqueness. PUFs are used in low cost authentication and secure key generation for cryptographic applications. Generally, Strong PUFs are used for authentication and weak PUFs are used for key generation. The PUF circuits will have inputs and outputs, generally referred as challenge and response respectively. The PUF circuits on different devices will have unique response for the same challenge due to internal manufacturing variability. Internal manufacturing variability of the PUF circuit in each device is unique, hidden and distinct.

The difference between weak and strong PUF is the number of unique challenge –response pairs (CRP's) it can process. Weak PUF support small number of CRPs and in few cases it may be only one pair. A strong PUF can support a large number of CRPs. For an ideal strong PUF, the measurement of all possible CRPs within a limited time frame is impossible. The different types of PUF circuits are proposed by researchers. The important ones are: SRAM PUF [17], Ring Oscillator (RO) PUF [18], Latch PUF [19], TERO PUF [20], Flipflop PUF [21] and Butterfly PUF [22]. The arbiter PUF and RO PUF circuits are most versatile PUF structures discussed and used in various applications. Out of several PUF architectures mentioned, we have to choose right PUF architecture for SST application. PUF construction which has a proven behavior in earlier experiments with large number of CRP pairs is chosen for SST. PUF used in SST is for authentication of the device and to implement the secure locking mechanism. In general, the quality of PUF is decided by the following properties: uniqueness, uniformity, reliability, and bit-aliasing. These are common properties used in PUF related literature.

Uniqueness: The ability of the PUF circuit to generate a unique response for a particular chip among the group of chips of same type for same stimulus. Hamming distance is used to measure the uniqueness. Uniqueness is an estimate of an inter chip variation of a PUF response.

Reliability: Reliability of the PUF is the ability of a PUF circuit to generate the same response for a given challenge repeatedly applied. The ideal value of reliability of a PUF circuit is 100%. Environmental conditions like temperature, supply voltages and other issues like aging of the CMOS gates will affect the reliability of the PUF circuit.

Uniformity: The estimation of the proportion of 0's and 1's in the PUF response. For an ideal PUF, the value of uniformity is 50%. Uniformity of a PUF is defined using percentage of the hamming weight of the response.

Bit –aliasing: The PUF circuit in the different chips produce nearly identical responses which is an undesirable effect. Bit-aliasing of n^{th} bit in the PUF response is calculated as the percentage hamming weight of the n^{th} identifier across k (total) devices.

The detailed description with equations used to calculate above mentioned properties can be found in [23] [24]. Abranil maiti and others in [23] study arbiter and ring oscillator PUF systematically and conclude that ring oscillator PUF is better than arbiter PUF with the comparison below:

Table 1: Comparison table between Arbiter PUF and RO PUF in [23]

	Ideal Value	Arbiter PUF	RO PUF
Uniqueness	50%	7.20%	47.24%
Reliability	100%	99.76%	99.14%
Uniformity	50%	55.69%	50.56%
Bit-aliasing	50%	19.57%	50.56%

RO PUF is a weak PUF and it has limited number of CRP pairs. The SST application needs a PUF with large number of CRP. Arbiter PUF is a strong PUF with large number of CRP's. It is evident from the table 1, that RO PUF has got better uniqueness and bit-aliasing properties than Arbiter PUF. The PUF proposed in [25], increased the number of CRP's for RO PUF without affecting the properties, but hardware overhead and design complexity is very high and not suitable for SST. Sahoo et.al in [26, 27] present the composite PUF, uses both arbiter PUF and RO PUF in the structure to retain the properties of RO PUF and achieved the large CRP space of arbiter PUF. The architecture of Composite PUF is shown in figure 3. The challenge to PUF is applied to RO-PUF first and responses of the RO-PUF will be used as challenge to the arbiter PUF internally. The response output of the arbiter PUF is the response of composite PUF. The results of composite PUF is presented in table 2. From table 2, it is observed that, the composite PUF is better than arbiter PUF. Composite PUF also have large CRP space. The bit –aliasing of composite PUF is not good in comparison with RO-PUF and other properties are acceptable. Uniqueness and Reliability are important properties required for SST. Composite PUF is a strong PUF with acceptable uniqueness and reliability, so in this work, composite PUF is used in SST.

Table 2: Properties of Composite PUF in [26]

	Ideal Value	Composite PUF
Uniqueness	50%	47.57%
Reliability	100%	90.70%
Uniformity	50%	47%
Bit-aliasing	50%	14.95%

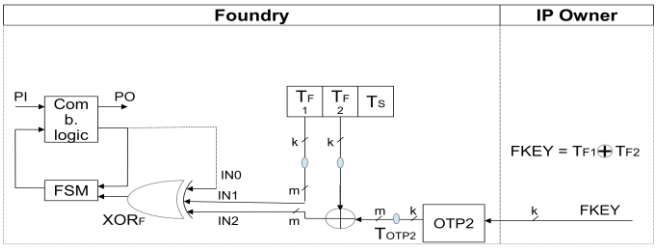

Figure 2 (a): Functional locking block in [12, 13]

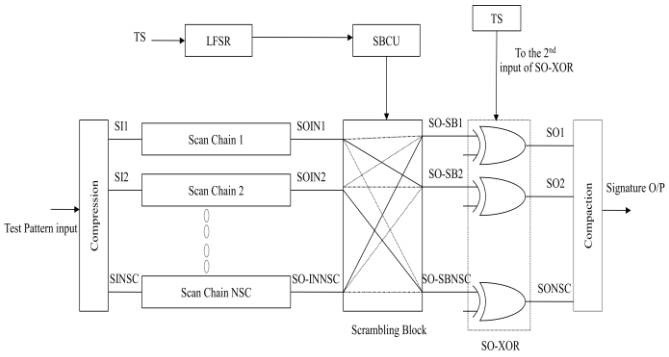

Figure 2 (b): Scan locking block in [12, 13]

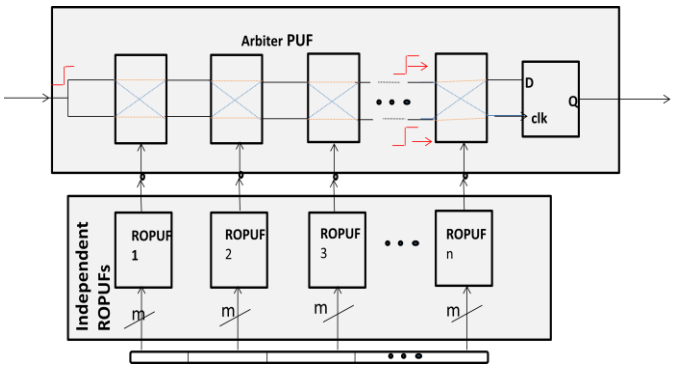

Figure 3: Composite PUF architecture [26]

IV. PHYSICAL UNCLONABLE FUNCTION BASED SECURE SPLIT TEST

A. Proposed Architecture:

The figure 4 shows the block diagram of the proposed architecture. PUF-SST Architecture comprises of composite PUF, Error Correcting Code (ECC) block for PUF responses, RSA blocks for PUF enrollment, Scrambler and Pseudo Random Number Generator (PRNG) for PUF challenge generation.

The operation of PUF-SST is as follows:

- PRNG inside the each chip start generating the input stimulus to composite PUF. The CRP's from the PUF are collected for 5000 clock cycles initially. In each clock cycle, one set of challenge-response pair is collected.
- After 5000 cycles, the test patterns for scan test are applied on the device and responses are scrambled. Signature is obtained from compaction block, which compress the scrambled scan output. Input to the scrambler logic to scramble the scan output comes from PUF. The output of the PUF at 5001 cycles is used for scrambling logic for scrambling the scan output.
- The signatures generated out of compression of scan out after scrambling and electronic chip ID (ECID) is sent to design house or original chip maker (OCM). The 5000 CRPs and 5001 CRP (used for scrambling) generated from PUF are encrypted using RSA and sent to design house. The design house will decrypt the RSA and find out scrambling logic to decode the signature. The device PASS/FAIL data is extracted from the signature.

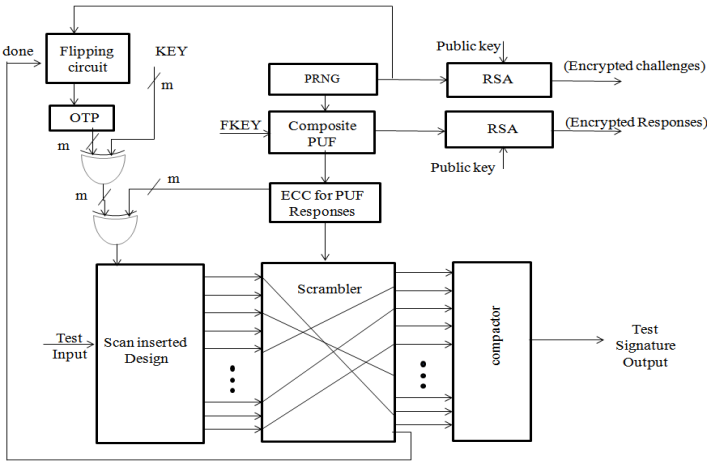

Figure 4: Proposed PUF based SST architecture

- The 5000 CRP's of PUF is collected and stored in a server for future device authentication purpose. Out of 5000 CRP's it is easy to find out the challenge (stimulus) to PUF which will generate the functional key to unlock the design. The more number of CRP's can be collected and their collection will depend on the number of chips manufactured.
- To perform functional testing, functional key is shared with ATP centre. By applying the functional key to PUF input, ATP centre will perform functional testing. Initially all values in the One-Time Programmable (OTP) memory is logic '1'. The XOR gates will act like NOT gate when one of the input is fixed as logic '1' and as buffer when input is fixed as logic '0'. ATP centre will apply FKEY to PUF and KEY (all zeros of length 'm'). Functional key generated by PUF will unlock the design for functional test through the XOR gate (which acts like a buffer). The same PUF response is used to scramble the test response. After functional test response is collected and scrambled completely, scrambling block generates the done signal. The signature for scrambled output is generated using compactor.
- The "done" signal generated by scrambling block triggers PRNG to generate some random bits. Random bits are flipped using flipping circuit and written into OTP. The same random bits generated by PRNG are encrypted using RSA block. The encrypted ECIDs, PRNG random bits and signature are communicated to design house. The design house de-scrambles and decodes the signature to decide the functional test result. The encrypted random bits generated from PRNG are decrypted. The flipping logic is known and design house derives the KEY. The design house will share the FKEY and KEY with customer directly after realization of random bits stored in OTP. The end user will apply FKEY and KEY to unlock the chip.

B. Scan locking:

Scan locking block is similar to CSST architecture, except the input to the scrambling block comes from PUF output.

C. *Functional locking:* Functional locking block is different from earlier SST designs. The proposed SST scheme needs changes in design for lock-unlock mechanism. The design will go into the functional mode only a specific input is applied at the inputs; otherwise it will stay in non-functional states. The output of PUF circuit will serve as key to unlock the design for functionality. For FSM based designs, lock-unlock mechanism is simple. This mechanism of locking/unlocking the design using PUFs is found in [28]. The FSMs with lock-unlock mechanism are called Boosted FSMs (BFSM). The 5000 CRPs are collected from PUF to identify the functional keys which generate the key to unlock the design for functionality from the PUF response.

D. *Communication flow between design house and ATP centre:* The communication flow between design house and ATP centre is as follows*:*

- Encrypted PUF CRPs, ECIDs and signature of Scan test output is communicated to design house from ATP centre.
- Pass ECIDs and their functional key (FKEY) are shared with ATP centre to perform functional test.
- The signature of functional test and encrypted PRNG random bits will be sent to design house from ATP centre.
- The design house or OCM will provide both FKEY and KEY to the end user.

E. *Discussion:*

- The proposed architecture is complicated in comparison with earlier SST architectures. This architecture requires two RSA encryption blocks. The composite PUF is large in area, when compared with TRNG and OTP based SST architecture proposed earlier.
- The number of CRPs collected in our work is 5000. The number of CRPs can even more or less depending on the number of chips produced and other requirements. There is no standard available for how many numbers of CRPs should be collected in device authentication and hardware metering schemes.
- The PUF implementation used for SST can be used for IP protection, cryptographic key generation in other applications, where device is used.
- The modification in design is required to implement proposed SST. Inclusion of Functional locking and unlocking mechanism into the design is required to support proposed SST. In earlier SST proposals, no design modification is required.
- According to the proposed scheme, the 5000 CRPs are collected from each device. This gives more strength to device authentication and identification mechanism during counterfeit litigation.
- Due to CRP collection, there may be increase in test time. The frequency of devices and test equipment (ATE) operates in the scale of MHz and it takes few milli seconds to collect required CRPs.
- The amount of data is higher due to large number of CRPs collected from PUF should get enrolled in designer or OCM database.

V. IMPLEMENTATION AND RESULTS

A. *Design of PUF-SST:* The construction of composite PUF is shown in figure 3. The n-bit challenge is divided into sub-challenges of each m-bit and applied to RO-PUF. The output response of RO-PUF will be fed into Arbiter PUF as challenge. The single bit response will be obtained from each composite PUF instance as shown in figure 3. In this experiment, 4 RO-PUFs and Arbiter PUFs are used in the construction of basic element of composite PUF. The composite PUF instance is implemented for 8 instances in the FPGA. The value of 'n' and 'm' is 16 and 4 respectively. The each RO-PUF will have 4-bit challenge and produce one bit response which internally gets fed into Arbiter PUF as a challenge. By applying 16-bit challenge to composite PUF, one bit response is obtained. For 8 instances of composite PUF, the same 16-bit challenge is applied to get 8-bit response. This means the PUF architecture will have 128-bit inputs (16 x8) and 8-bit output (from each PUF instance). The 16-bit PRNG circuit is implemented. The 8 instances of 16-bit PRNG are used to drive the PUF. The RSA blocks, PUF and other supporting circuits are designed using Verilog HDL. The scrambling block used in earlier SST techniques [12, 13] is used in this design also. The input to the scrambling block can be equal to the number of scan chains in the design. The number of scan chains will be more for large designs, in such cases only few scan chains can be selected for the scrambling. The number of inputs to scrambler can be decided by the designer according to the requirement. In this work, we have taken s38417 and s35932 benchmarks from ISCAS'89. The number of scan chains in s38417 and s35932 is 10.

B. *Results:* The number of scan chains used in both the benchmarks is 10. For a varying Scrambling block input (N_{SB} = 2 means only two scan outputs are used for scrambling and rest 8 scan outputs are directly passed to compactor for signature generation) the hamming distance analysis for between CSST in [12] and proposed PUF-SST is presented in Table 3. The hamming distance is measure for security and ideal value of Hamming distance is 50%. From Table 3, we can observe that, the difference in hamming distance results obtained for PUF-SST is comparable with CSST presented in [12]. The hamming distance analysis for functional key (FKEY) to unlock the design is shown in Table 4. The FKEY hamming distance is calculated on 10 FPGA chips.

C. *Security Analysis:* The proposed PUF-SST is resilient to attacks described in [13]. The foundry does not have any information on the length of the PUF response. The functional locking mechanism is more secure than SST proposed in [13]. The tampering attack requires bypassing the outputs from PRNG, which is expensive. FKEY and KEY are different for different chips. Performing the tampering operation on single chip is expensive. FKEY is known to ATP centre even for functionally faulty chips. To unlock the functionality, user also needs KEY. KEY is not known to ATP centre. So the faulty chips entering supply chain from untrusted ATE can be avoided.

Table 3: Hamming Distance (HD %) comparison for CSST and PUF-SST

NSB	CSST in [12] (s38417)	Proposed PUF-SST	
		s38417	s35932
2	42.24	40.6	41.23
4	44.59	44.8	45.12
10	50.03	49.8	50.31

.

Table 4: Hamming Distance analysis for FKEY

	s38417	s35932	Ideal Value
Hamming Distance (HD) %	44.52%	43.3%	50%

VI. CONCLUSION

Secure Split Test (SST) is a technique which facilitates the IP owners or OCM to involve in production testing process, so that counterfeit chips coming out from untrusted ATP centers can be mitigated. An improved model of SST is Connecticut Secure Split-Test (CSST). Both SST and CSST do not include functional tests in the production testing, which is critical in recent times to weed out faulty chips. To address this issue, we propose a novel Physical Unclonable Function (PUF) based SST technique which support functional testing of chips without compromising the security features of CSST. This PUF-SST designed for packaged parts and in future work, we will incorporate the wafer probing to make the solution for hardware metering acceptable to industry.

REFERENCES

[1] Rostami M, Koushanfar. F, Karri. R, "A Primer on Hardware Security: Models, Methods, and Metrics", *Proceedings of IEEE*, Vol. 102, Issue – 8, pp. 1283-1295, Aug 2014.

[2] Nicole Faubert, http://www.edn.com/electronics-blogs/all-aboard-/4426389/Counterfeit-threats-for-electronic-parts, -December 30, 2013

[3] U. Guin et al., "Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead," Journal of Electronic Testing, vol. 30, pp. 9-23, 2014.

[4] H. Livingston, "Avoiding Counterfeit Electronic Components", IEEE Transactions on Components and Packaging Technologies, vol. 30, pp.187-189, 2007.

[5] "Defense Industrial Base Assessment: Counterfeit Electronics", http:// www.bis.doc.gov, U.S. Department of Commerce Bureau of Industry and Security Office of Technology Evaluation, 2010.

[6] J. Stradley and D. Karraker, "The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications", IEEE Transactions on Components and Packaging Technologies, vol. 29, num. 3, pp.703-705, 2000.

[7] K. Chatterjee and D. Das, "Semiconductor Manufacturers Efforts to Improve Trust in the Electronic Part Supply Chain", IEEE Transactions on Components and Packaging Technologies, vol. 30, num. 3, pp.547-549, 2007.

[8] G.E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", in proc. 44th ACM/IEEE Design Automation Conference (DAC '07), pp.9-14, 2007.

[9] Y.M. Alkabani and F. Koushanfar, "Active hardware metering for intellectual property protection and security", in proc. 16th USENIX Security Symposium, pp.20:1-20:16, 2007

[10] J.A. Roy, F. Koushanfar, and I.L. Markov, "EPIC: Ending Piracy of Integrated Circuits", in proc. Design, Automation and Test in Europe 2008 (DATE '08), pp.1069-1074, 2008.

[11] G. Contreras, M. T. Rahman, and M. Tehranipoor, "Secure Split-Test for Preventing IC Piracy by Untrusted Foundry and Assembly," in Int.Symposium on Defect and Fault Tolerance in VLSI Systems, 2013.

[12] Md. Tauhidur Rahman et al., "CSST: An Efficient Secure Split-Test for Preventing IC Piracy," In IEEE North Atlantic Test Workshop, May-2014.

[13] Md. Tauhidur Rahman, Domenic Forte, Quihang Shi, Gustavo K. Contreras, and Mohammad Tehranipoor CSST: Preventing Distribution of Unlicensed and Rejected ICs by Untrusted Foundry and Assembly, International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)-October- 2014

[14] Jeroen Delvaux, Dawu Gu, Dries Schellekens, Ingrid Verbauwhede "Secure Lightweight Entity Authentication with Strong PUFs: Mission Impossible? "Lecture Notes in Computer Science Volume 8731, pp 451-475, Cryptographic Hardware and Embedded Systems – CHES 2014

[15] F. Koushanfar, G. Qu, M. Potkonjak, "Intellectual Property Metering", in proc. 4th International Workshop on Information Hiding (IHW '01), pp.81-95, 2001.

[16] Majzoobi, Koushanfar, Potkoniak, "Techniques for Design and Implementation of Secure Reconfigurable PUFs", ACM Transactions on Reconfigurable Technology and Systems (TRETS), Vol.2, Issue 1, Article No.5, March 2009.

[17] Garg, A.,Kim, T.T. , "Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect", Pages1941 – 1944, IEEE International Symposium on Circuits and Systems (ISCAS) June 2014

[18] Abranil Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-Friendly Secure Primitive", *IACR Journal of Cryptology*, vol. 24, issue 2, April, 2011, pp. 375-397.

[19] Yamamoto, D.; Sakiyama, K.; Iwamoto, M.; Ohta, K.; Takenaka, M. & Itoh, K. "Variety enhancement of PUF responses using the locations of random outputting RS latches Journal of Cryptographic Engineering, Springer Berlin Heidelberg, 2013, 3, 197-211.

[20] Bossuet, L. Xuan Thuy Ngo ; Cherif, Z. ; Fischer, V." A PUF Based on a Transient Effect Ring Oscillator and Insensitive to Locking Phenomenon " IEEE Transactions on Emerging Topics in Computing, Volume:2 , Issue: 1 Pages:30 – 36, October 2013.

[21] Simons, P. van der Sluis, E. ; van der Leest, V. "Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs" **,** IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Pages 7 - 12 ,June 2012 .

[22] Kumar, S.S. Guajardo, J. ; Maes, R. ; Schrijen, G.-J. ; Tuyls, P. "The butterfly PUF protecting IP on every FPGA" IEEE International Workshop on Hardware-Oriented Security and Trust (HOST) June 2008 Pages67 - 70 .

[23] Abhranil Maiti, Vikash Gunreddy, Patrick Schaumont "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions". IACR Cryptology ePrint Archive, 657, 2011.

[24] Y.Hori**,** T.Yoshida, T.Katashita, and A.Satoh, Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs, 6th International Conference on ReConFigurable Computing and FPGAs (ReConFig'10), Cancun, Quintana Roo, Mexico, Dec. 13-15, 2010. pp.298-303.

[25] Abhranil Maiti, Inyoung Kim, Patrick Schaumont, "A Robust Physical Unclonable Function With Enhanced Challenge-Response Set" IEEE Transactions on Information Forensics and Security, 2012

[26] Sahoo, D.P. Mukhopadhyay, D. ; Chakraborty, R.S. "Design of low area-overhead ring oscillator PUF with large challenge space" International Conference on Reconfigurable Computing and FPGAs (ReConFig)- Dec. 2013 Pages 1 – 6.

[27] Sahoo, D.P. Saha, S. ; Mukhopadhyay, D. ; Chakraborty, R.S. ; Kapoor, H., "Composite PUF: A new design paradigm for Physically Unclonable Functions on FPGA "IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), May 2014, Pages 50 - 55

[28] Rajat Subhra Chakraborty, Swarup Bhunia, HARPOON: an obfuscation-based SoC design methodology for hardware protection, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems-2009. Volume-28, Issue-10, Pages 1493-1502.

[29] Guin, U. Chakraborty, T. ; Tehranipoor, M., Functional Fmax test-time reduction using novel DFTs for circuit initialization, IEEE 31st International Conference on Computer Design (ICCD), Oct. 2013

[30] Bernardi, P. Ciganda, L.M. ; Sanchez, E. ; Reorda, M.S., MIHST: A Hardware Technique for Embedded Microprocessor Functional On-Line Self-Test IEEE Transactions on Computers, Volume:63 , Issue: 11 Pages 2760 – 2771, 15 August 2013.