PUF-based Secure Test Wrapper Design for Cryptographic SoC Testing

Amitabh Das *, Ünal Kocabaş **, Ahmad-Reza Sadeghi ***, and Ingrid Verbauwhede *
* K.U. Leuven, ESAT/COSIC, Leuven, Belgium
{amitabh.das, ingrid.verbauwhede}@esat.kuleuven.be
** System Security Lab, TU Darmstadt/CASED, Germany
unal.kocabas@trust.cased.de
*** System Security Lab, TU Darmstadt/CASED and Fraunhofer SIT, Darmstadt, Germany
ahmad.sadeghi@trust.cased.de

Abstract—**Globalization of the semiconductor industry increases the vulnerability of integrated circuits. This particularly becomes a major concern for cryptographic IP blocks integrated on a System-on-Chip (SoC). The trustworthiness of these cryptographic blocks can be ensured with a secure test strategy. Presently, the IEEE 1500 Test Wrapper has emerged as the test standard for industrial SoCs. Additionally a secure activation mechanism has been proposed to this standard in order to restrict access to the testing interface to eligible testers by using a cryptographic authentication mechanism. This access mechanism is necessary in order not to provide any side-channels which may leak secret information for attackers. However, this approach requires the authentication mechanism to be implemented in hardware incurring an area overhead, and the authentication secrets to be securely stored in non-volatile memory (NVM), which may be susceptible to side-channel attacks. In this work, we enhance the secure test wrapper allowing testing of multiple IP blocks using a PUF-based authentication mechanism which overcomes the necessity of secure NVM and reduces the implementation overhead.**

Keywords- Secure Test Wrapper; Scan Chains; SoC Testing; Physically Unclonable Functions (PUF)

I. INTRODUCTION

Today as a result of globalization, the development and fabrication of advanced integrated circuits (ICs) is typically migrating offshore. This migration to third-party providers and to low-cost foundries has made ICs vulnerable to security compromise, functional changes, information leaks or even system failures under specific conditions. Such intrusions may pose a major threat to embedded systems in critical applications and infrastructures. These risks have been considered not only in the academic community but also in the fabless semiconductor industry and governmental agencies. In this context, secure testing environments are becoming more important in ensuring a trustworthy hardware environment.

System-on-Chip (SoC) integrators often use embedded cores which may be procured externally from various IP vendors. Standard functional testing or Design for Testability (DFT) methods cannot be employed directly for IP testing in SoCs. The security of an SoC depends on the resistance of these IP cores to attacks exploiting the existing on-chip DFT. Particularly, cryptographic IP cores, such as AES and RSA implementations, must be protected from such attacks. Due to the possible attack scenarios on SoCs, the customers need to securely test the individual cryptographic IP blocks after the deployment of SoCs.

Cryptographic SoC testing can be provided by a two-step approach: scan-chain and Built-in-Self-Test (BIST). Scan chains protected through a custom test wrapper interface can be employed for functional and structural testing of each IP block after SoC integration. BIST can be used for runtime testing of a complete SoC in the field during normal operation. Normally, BIST should not be used for testing each IP block separately due to its relatively high area overhead requirement. However, BIST only provides a pass/fail output which is not useful for diagnosis. Hence, in this paper, we focus on scan chains to achieve high testability for each IP block.

In [1], the high testability of scan chains has been combined with a secure Test Wrapper to achieve restricted access with reasonable test area overhead. This has been achieved using a light-weight block cipher to activate an unlocking mechanism for the test wrapper, to allow direct access to cryptographic IP blocks on the tester equipment by scan chains. The authentication mechanism with the block cipher requires additional non-volatile memory (NVM) to store the secret key, which may be susceptible to side-channel analysis.

Contribution: In this paper, we propose a PUF-based secure test wrapper which provides a secure test environment allowing only eligible testers to test the individual IP blocks in a SoC. The requirement of secure-key storage on NVM is overcome by using a Hamming distance-challenge based authentication mechanism using physically unclonable functions (PUFs) in order to prevent replay attacks.

Outline: After presenting a brief summary of PUFs and the secure test wrapper in section II, we introduce the adversary model and the concept of the activation mechanism of the secure test wrapper and the security of the protocol in section III. The implementation details and results are given in section IV. We conclude the paper and discuss future work in section V.

978-3-9810801-8-6/DATE12/ ©2012 EDAA
This work has been supported in part by the European Commission under grant agreement ICT-2007-238811 UNIQUE and in part by the IAP Programme P6/26 BCRYPT of the Belgian State. * Amitabh Das is funded by a fellowship from Erasmus Mundus External Cooperation Window Lot 15.

II. BACKGROUND AND RELATED WORK

A. Physically Unclonable Functions (PUFs)

PUFs are promising security primitives that exploit the physical characteristics of a device. PUFs can be used as secure key storage [2],[3] and in authentication protocols [4],[5]. A stimulus applied to a PUF is called challenge C, and the reaction of the PUF is called response R. The response depends on both the challenge and the unique intrinsic randomness of the device. Since PUFs are based on the physical properties of the device in which they are embedded, no other entity can verify the response of a PUF to a given challenge without a priori knowledge of an authentic Challenge Response Pair (CRP).

Typical assumptions on PUFs are [6]:

- *Unpredictability*: An adversary cannot predict the response to a challenge of a specific PUF. Moreover, the response R_i of one CRP (C_i,R_i) gives only a negligible amount of information on the response R_j of another CRP (C_j ,R_j) with $i \neq j$.
- *Unclonability*: An adversary cannot emulate the behavior of a PUF on another device since the behavior is fully dependent on the physical properties of the original device.
- *Tamper-resilient*: Any physical attack against a PUF will irreversibly and randomly change its challenge-response behavior.
- *Robustness*: For a single PUF, the difference between two responses of a particular challenge should be small.

Among different PUF architectures, we focus on silicon PUFs, which can be easily applied to ICs. In particular, we consider Arbiter PUFs (APUFs) [7] which are based on race conditions on two identical logic paths. Independent of the semiconductor manufacturing technology, there are inevitable variations in the propagation delays of logic paths. If one implements two identical logic paths which are controlled by a challenge and get triggered simultaneously, due to different propagation delays, one transition occurs first. A digital arbiter captures this transition and indicates which of the two signals was the fastest and therefore produces a one-bit response. By using a challengeable logic path, the number of responses of a single APUF can be made exponentially large in the dimensions of the APUF (large CRP source), which makes them a good candidate to be used in authentication mechanisms. However, it was shown in [8] that APUFs are subject to model building attacks that allow predicting responses with non-negligible probability. Further, the response of APUF cannot be used directly as a key in an authentication mechanism without post-processing, since APUF responses are obtained through measurements which suffer from inevitable environmental noise. Two queries of the same challenge may give different responses and eventually the authentication mechanism does not work properly. In order to counter these problems, additional primitives must be used: controlled PUFs [9] use cryptography in hardware to hide the responses of the underlying PUF from an attacker and fuzzy extractors (FE) [10] correct the errors in PUF responses.

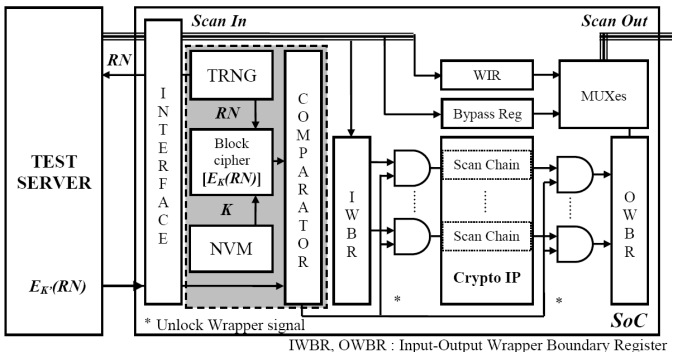

Figure 1. Secure Test Wrapper architecture [1]

B. Secure Testing and SoC Integration Testing Environment

DFT infrastructure is usually fabricated in all chips to aid the testing process. The DFT infrastructure may involve scan chains which provide highest testability, but are insecure against scan-based side-channel attacks. There have been attacks on both DES and AES implementations exploiting only the scan-chains [11], [12]. An alternative approach can be Built-in-Self-Test (BIST) which provides high security. In this approach, test inputs are generated internally by a Pseudo-Random Pattern Generator, responses are compacted by a Multiple Input Signature Register and then these responses are compared with a stored golden signature of the circuit. But it entails relatively high test area overhead and only provides a pass-fail signature which is not useful for diagnosis. There is always a trade-off between security, testability and test cost in all secure testing approaches for cryptographic circuits.

There have been many approaches at secure DFT. The scan chain scrambling technique, presented in [13], randomizes the scan chain data by performing a pseudo-random selection of scan chains to be loaded at a time through a Linear Feedback Shift Register (LFSR) and a MUXed structure. In the Lock and Key Technique [14], the scan chains are divided into a number of sub-chains. The access to these sub-chains is controlled through a Test Security Controller (TSC) which randomizes their operation in case of an unauthorized access by an attacker. Design for Secure Test (DFST) [15] provides a testing solution targeting the round structure of AES in particular. The approach taken in [16] uses a modified IEEE 1149.1 Boundary Scan controller that resets the chip and removes all traces of any secret information or cryptographic algorithm in test mode. The Flipped Scan Tree architecture [17] obscures the scan design through the introduction of inverters at the scan-in input of some of the Scan D Flip-Flops. However, these secure testing methods involve changes in the existing on-chip DFT or work only with specific cryptographic implementations. Hence, they may not be suitable for SoC integration where individual IP blocks needs to be included in the SoC generically, without internal modifications.

The secure test wrapper architecture in Figure 1, is constructed with a challenge - response based test protocol using a light-weight block-cipher. The authentication protocol seeks matching response values and executes with the following steps: First, True-Random-Number-Generator (TRNG) generates a nonce value and sends this value to the on-

chip block cipher and also the test server. Both parties share the same block cipher and generate the same ciphertexts according to their secret keys. Only if these ciphertexts match, the protocol enables the scan-based testing environment of the crypto IP through the wrapper [1]. Otherwise the protocol rejects any attempts for testing the IP block.

III. PUF-BASED SECURE TEST WRAPPER (STW)

We propose an alternative secure test wrapper activation using a PUF-based authentication mechanism. This mechanism avoids key management of secret keys between parties, and allows only eligible tester to use the STW by using a CRP database of the underlying PUF.

A. Trust Model and Assumptions

As in most PUF based authentication schemes, we assume that the adversary can eavesdrop the communication channel and manipulate the messages exchanged with the SoC. However, similar to the PUF-based key storage [7], we assume that the adversary cannot access the response of the PUF. In our trust model, we are considering a SoC integration scenario; where the manufacturer is assumed to be trusted and the adversary cannot access the CRP database of underlying PUF. In addition the internal communication within the SoC is assumed to be secure.

B. Secure Test Wrapper Activation Mechanism

Every PUF-based authentication mechanism requires an enrollment phase in order to create a CRP database CRP_{SOC}. Figure 2 shows the enrollment mechanism. The manufacturer queries randomly chosen challenges depending on the CRP space size (0 to x) and stores the challenge-response pairs (C_i,R_i). In normal mode, our design prohibits listening to response values in order to prevent model-building attacks [8]. Therefore, after creation of CRP_{SOC}, the manufacturer disables read-out of PUF responses, e.g. by blowing fuses.

To prevent replay attacks, we propose a new mechanism expecting two challenges whose responses have a specific Hamming-distance. Figure 3 presents the authentication mechanism: First, the test server starts the protocol by sending a synchronization "SYN" signal to activate the Pseudo Random Number Generator (PRNG) which will create the random number $\Delta \neq 0$. This Δ value refers to the Hamming distance between two responses of the intrinsic PUF of the SoC. At this point, the server will check the database and find two responses (R_i,R_j) which have Hamming distance "Δ". Accordingly, (C_i,C_j) are sent by the test server to the SoC in order to authenticate that the tester owns the right to enable the testing environment of an IP block on the SoC. If the SoC PUF generates responses within few errors than can be corrected, then the IP block will be enabled for testing using scan chains. Otherwise, the mechanism fails and does not allow the test server to test the IP block. Finally, SoC sends an acknowledgment signal "ACK" back to the test server to indicate the authentication status.

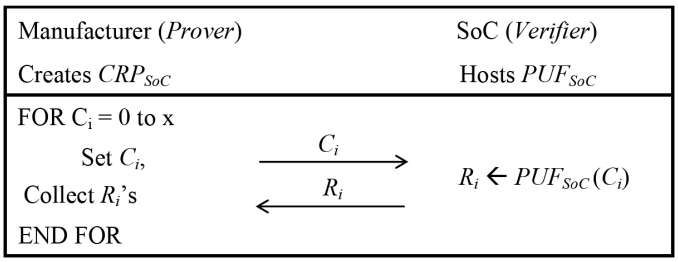

Figure 2. Enrollment of CRP database

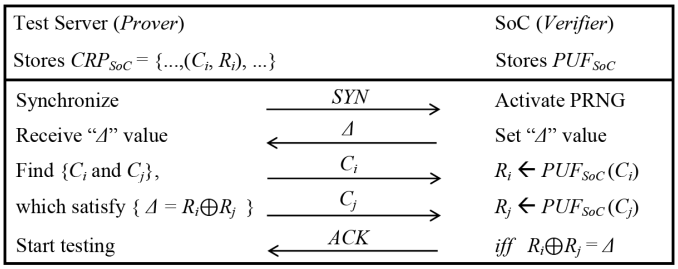

Figure 3. PUF-based Secure Test Wrapper Protocol

The size of CRP_{SOC} x is dependent on the bit length l_Δ of Δ. The argument of the size of required "x" to guarantee the matching "Δ" condition can be formalized as follows:

Assuming that PUF responses are uniformly distributed over $\{0, 1\}^x$ and for each of these responses there is precisely one challenge. Then the probability that a randomly chosen Δ in $\{0, 1\}^{l\Delta}$ can be constructed by the XOR of two values in CRP_{SOC} is:

$$({}^{x}C_2 + 1)2^{-l\Delta} \cdot (1 - x.2^{-l\Delta}) = 1 \qquad (1)$$

C. Security of the Mechanism

The security of the scheme depends on the ability of the adversary to predict the response of the PUF values by observing the communication taking place between the SoC and the test server. The adversary can make a list of (C_i, C_j, Δ) pairs to mount a replay attack or to predict (C_i, C_j) for an unknown Δ'. As long as Δ is selected large enough and because of unpredictability of PUF, the probability of success is negligible. In order to prevent reuse of the same Δ, a mechanism reseeds the PRNG (LFSR) after every authentication process. Specifically for this design, we recommend the use of 32-bit LFSR module and 64-bit PUF challenges.

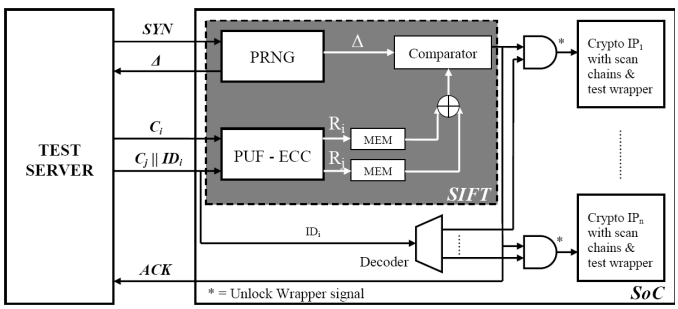

Figure 4. PUF-based Secure Test Wrapper Model

IV. Implementation and Comparison

The implementation of this authentication mechanism is given in Figure 4. The Secure Infrastructure for Test (SIFT) includes a PUF followed by an error-correction module[18], two registers (MEM) to store corresponding responses, XOR gates and two LFSRs. The error-correction module (ECM) is selected as a simple majority voting mechanism for 11-bits. In this way we corrected the errors of the PUF up to 5-bits. A 32-bit LFSR is implemented to generate Δ, and a 64-bit LFSR is implemented for session challenges of the PUF.

We compared the hardware area overhead of our PUFbased STW with a KATAN-64 based STW, which provides equivalent security to the 64-bit length PUF challenges used in our design. The results are shown in Table I. All area results are provided in gate equivalents (GE) of 2-input NAND gates for a Faraday 130 nm library, synthesized in Synopsys Design Compiler v2009.06, in conjunction with Synopsys DFT Compiler. The results show that the PUF-based STW is more efficient in terms of area requirements than the KATAN block cipher based implementation.

V. Conclusion

We presented a novel PUF-based Secure Test Wrapper scheme, which provides high testability and security to cryptographic IP blocks in a SoC integration scenario. Our approach is the first to propose the idea of using two challenge response pairs to compute the Hamming distance for an on-chip comparison, with a view to prevent replay attacks. This flexible test method is highly generic and works for all flavors of cryptographic implementations. Our implementation is more efficient in area consumption than previous designs and does not require secure NVM. For future work, we are expanding the scope of this secure test method for hardware Trojan detection and IP protection.

TABLE I. Area Comparison of the two Secure Test Wrappers

Design	*KATAN based**	*PUF based*
AES Implementation	17495	17495
With Normal Scan	18985	18985
With Scan and Std. Test Wrapper	23934	23934
With Scan and Secure Teset Wrapper	28932	26988
Overhead over Std. Test Wrapper	20.88%	12.76%

* Requires additional 80-bit NVM for key storage

Acknowledgment

We thank Roel Maes, Andreas Peter and Christian Wachsmann for their useful comments.

References

[1] A. Das, M. Knezevic, S. Seys, and I. Verbauwhede, "Challenge-response based secure test wrapper for testing cryptographic circuits," 16th IEEE European Test Symposium 2011 (ETS), 2011.

[2] B. Škori´c, P. Tuyls, and W. Ophey, "Robust key extraction from physical uncloneable functions applied cryptography and network security," Applied Cryptography and Network Security (ACNS) 2005.

[3] D. Lim, J. W. Lee, B. Gassend, E. G. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Transactions on Very Large Scale Integration (TVLSI), vol. 13, no. 10, pp.1200–1205, Oct. 2005.

[4] E. G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," ACM/IEEE Design Automation Conference (DAC) 2007.

[5] E. Öztürk, G. Hammouri, and B. Sunar, "Towards Robust Low Cost Authentication for Pervasive Devices," International Conference on Pervasive Computing and Communications (PERCOM), Mar. 2008.

[6] R. Maes, and I. Verbauwhede, "Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions," In Towards Hardware-Intrinsic Security, Security and Cryptology, D. Naccache, and A. Sadeghi (eds.), Springer, 2010.

[7] D. Lim, "Extracting Secret Keys from Integrated Circuits," IEEE Transactions on Very Large Scale Integration (TVLSI) Systems, 2004.

[8] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," ACM Conference on Computer and Communications Security (ACM CCS) 2010.

[9] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled physical random functions," Computer Security Applications Conference (ACSAC). IEEE, 2002, pp. 149–160.

[10] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other noisy data," EUROCRYPT 2004.

[11] B. Yang, K. Wu, and R. Karri, "Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard," Proceedings of the IEEE Int. Test Conf. (ITC), 2004, pp. 339–344.

[12] B.Yang, K. Wu, and R. Karri, "Secure Scan: A Design-for-test Architecture for Crypto Chips," Design Automation Conference (DAC), 2005.

[13] D. Hély, M.-L. Flottes, F. Bancel, and B. Rouzeyre, "Scan Design and Secure Chip," International On-Line Testing Symposium (IOLTS), 2004.

[14] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellice, "Securing Designs against Scan-Based Side-Channel Attacks," Transactions on Dependable and Secure Computing, Vol. 4, No. 4, 2007.

[15] Y. Shi, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "Design for Secure Test - A Case Study on Pipelined Advanced Encryption Standard," ISCAS, 2007.

[16] D. Hély, F. Bancel, M.-L. Flottes, and B. Rouzeyre, "Test Control for Secure Scan Designs," European Test Symposium (ETS), 2005.

[17] G. Sengar, D. Mukhopadhayay, and D. R. Chowdhury, "An Efficient Approach to Develop Secure Scan Tree for Crypto-Hardware," International Conference on Advanced Computing and Communications, 2007.

[18] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," SIAM J. Comput., vol. 38, no. 1, pp. 97–139, 2008.