Adit D. Singh, Ph.D.
Godbold Endowed Chair Professor
Auburn University
Auburn, AL 36849
adsingh@auburn.edu

June 10, 2024

Reviewer's opinion
on Ph.D. dissertation authored by

Bartosz Wlodarczak

entitled:

On Secure Deterministic In-System Test Solutions

1. Problem and its impact

What is, in your opinion, the most important problem discussed in the dissertation?

This dissertation addresses challenges in the the broad area of reliable computing. In particular, it is focused on the efficient and effective testing of computing circuits to screen out ICs and SoCs with fabrication defects post manufacture, and in-system testing in operation to also detect failures in the field.

Is it a scientific one? Does it have a practical meaning?

With the ubiquitous growth in the deployment of safety critical autonomous systems, increasing controlled by artificial intelligence, there is an obvious need for highly reliable hardware (and software). The test techniques developed in this dissertation present real advances that have been validated on complex industrial designs. The candidate has had the rare opportunity, for a student, to work closely with the top members of the technical staff at Siemens DIS, the leading electronic design automation company in digital circuit testing. This is reflected in the high quality of this research which is motivated by very real and practical test and reliability challenges being faced by computer chip manufacturing companies working with advanced state-of-the-art technology.

2. Contribution

What is the main, original contribution of the dissertation?

There are two broad related areas in which this dissertation has made significant original contributions: (1) test compression for improved IC testing efficiency, and (2) hardware security employed to protect intellectual property (IP) associated with the part being tested by encrypting test data. This is especially important when testing is outsourced to third parties, as is common.

In the area of test compression, the contributions here are improved X-masking designs/architectures for test result compaction for both traditional logic BIST, as well as for Deterministic In-System Test (DIST), which is a new application rapidly gaining importance for the periodic testing of ICs during in-field deployment in critical applications. Testing large ICs and SOCs requires very large sets of test stimulus data and the corresponding "correct" expected output data. These can require long test times to get in and out of a chip with typically limited I/O bandwidth. Consequently, both input and output data sets must be significantly compressed (typically ~100X with obvious information loss) to reduce test time. This thesis focuses on test output compaction, i.e. combining a large number of bits which are the results of the test applied using on chip hardware to generate an output signature that gets corrupted if there is an error in one or more of the compressed bits. However, unknown X logic values in the design (arising from uninitialized flip-flops, floating outputs of tri-state gates, marginal timing false paths, etc.) which are unavoidable, can make the correct signature nondeterministic and unpredictable, resulting in loss of test coverage. One solution is to mask out the X bits at the input of the compactor whenever they occur, by using additional hardware, along with mask data associated with every test pattern. However this can incur a very high overhead. Consequently, current approaches can mask out only a limited number of X values in any test response. Many X values find their way into the compacted output resulting in test inefficiencies. The X-masking approach developed in this thesis is able to handle a larger number of X values, including in new observation scan designs that capture errors in every scan shift cycle in an attempt to significantly reduce test pattern counts. This is latter approach is particularly important for new DIST applications.

In the area of hardware security, the contributions in this dissertation address the need for obscuring and thereby protecting intellectual property associated with the part being test. This can be compromised if uncoded test input and output sequences are available to an adversary. Such concerns arise if post manufacturing testing is outsourced to an untrusted third party. The obvious solution is to robustly encode the scan test data as it flows in and out of the device being tested. However, the coding must be simple enough to be quickly decoded and encoded on chip, with low hardware overhead, so as not to slow down the test flow. More critically, any decoding keys stored in the IC must be fully protected. This research presents innovative lightweight cryptographic primitives which can be used to build a hardware "root of trust" to protect this information in the scan test infrastructure, and thereby protect design IP against malicious attacks. The proposed approach is designed to work in conjunction with the new streaming scan network (SSN) architecture for SOC test access and appears to be forward looking and practical.

As mentioned earlier, this work is both important and highly practical because of candidate's unique access to experts working on cutting edge industrial technology in the field. His Ph.D. supervisors are inventors of the widely used test compression technology; Dr. Rajski has led test development at Siemens for over 30 years. Consequently, the motivation and guidance of this research is exceptional. In addition, the candidate has performed extensive simulation experiments on a large number of industrial designs that he has access to through Siemens to validate the research results. The experimental results presented here give me confidence that the solutions here are practical.

3. Correctness

Can we trust what is claimed in the dissertation? Are the arguments correct? Indicate the flaws you have noticed, if any. Also point out those aspects concerning correctness that you value most.

As best as I can tell everything seems to be technically sound and correct. The writing is exceptionally good, and the arguments are very well made. All the major contributions have been reviewed and published in 5-6 journal papers in the IEEE Transactions on Computers or Transactions in CAD, with additional conference publications. If I have any issue with the dissertation, it is that the content is quite dense -it takes time to develop an intuitive sense on where the benefits of the various scheme are coming from. This is likely because the problems addressed are not purely conceptual, but also very practical and design dependent.

4. Knowledge of the candidate

The candidate has displayed excellent knowledge of the general field of computing, and also the published research with respect of the specific problems that he has addressed. Prior work on X-masking and X-tolerant compactors is extensively reviewed and explained in Chapter 2. The early sections of Chapter 3 and 4 describe the context of the specific test compression architectures that are the target of the proposed new X-masking designs. Similarly, Chapter 5 presents prior work on security approaches to secure the scan testing, and reviews cryptographic hash functions and ciphers. Chapter 6 reviews LFSRs, ring generators and hybrid ring generators towards the development of the lightweight cryptographic primitives and root of trust presented in the later chapters.

All this prior research is very well described. The list of over 200 references is very comprehensive and appears to cover all the relevant research.

5. Conclusion

Taking into account what I have presented above and the requirements imposed by Article 13 of *the Act of 14 March 2003 of the Polish Parliament on the Academic Degrees and the Academic Title* (with amendments)[1], my evaluation of the dissertation according to the three basic criteria is the following:

A. Does the dissertation present an original solution to a scientific problem? (the selected option is marked with **X**)

☒	□	□	□	□
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

B. After reading the dissertation, would you agree that the candidate has general theoretical knowledge and understanding of the discipline of **Computing**, and particularly the area of **Software Engineering**?

☒	□	□	□	□
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

C. Does the dissertation support the claim that the candidate is able to conduct scientific work?

☒	□	□	□	□
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

Moreover, taking into account the fact that the research address real industry problems and the solutions appear to be extremely well developed and practical, I **recommend to distinguish** the dissertation for its quality[2].

ADSingh

Signature

[1] http://www.nauka.gov.pl/g2/oryginal/2013_05/b26ba540a5785d48bee41aec63403b2c.pdf

[2] Obviously, this sentence is optional.