UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

UNIVERSITÄT PADERBORN | 33095 PADERBORN

FAKULTÄT FÜR ELEKTROTECHNIK,
INFORMATIK UND MATHEMATIK

Institut für Elektrotechnik und
Informationstechnik
Fachgebiet Datentechnik

Prof. Dr. Sybille Hellebrand
E-Mail: sybille.hellebrand@uni-paderborn.de

Report on the Thesis

"On New Class of Test Points and their Applications"

submitted by Justyna Zawada

In her thesis Justyna Zawada investigates several new applications for test point insertion and presents the respective algorithms together with comprehensive case studies. In my opinion, this work will have significant impact as outlined in the following. Since recent manufacturing technologies come along with complex defect mechanisms, previous gate level abstractions are no longer sufficient for achieving a high test coverage, and advanced test generation approaches also take into account lower level information. This, in turn, may lead to increased test pattern counts and test data volume. As known from the literature, test point insertion can improve the controllability and observability of internal nodes, and thus help to tackle the test generation problem. However, standard approaches for test point insertion target random pattern testability and do not consider the specific requirements of automatic test pattern generation (ATPG). In this context Justyna Zawada presents solutions for four different application domains, the details of which are discussed in the sequel.

The manuscript describes the work in seven chapters. To motivate the problem, the first chapter sketches typical test scenarios and their associated challenges. After explaining the problem of complex defects in modern manufacturing technologies, Justyna Zawada introduces scan-based test using external ATPG patterns, test data compression, pseudo-random built-in self-test (BIST), and hybrid test solutions with both pseudo-random and ATPG patterns. Finally, she also discusses security threats related to the test infrastructure, such as counterfeits of intellectual property. Then she clearly states the contributions of her thesis. She has developed new approaches for test point insertion targeting conflict resolution in ATPG, both improved ATPG pattern count and random pattern testability in hybrid test, increased observability in a capture-per-cycle scan-based BIST scheme, as well as counterfeit protection by logic blocking. The introduction closes with an overview of the organization of the work.

Chapter 2 provides the necessary background in testing and also points to the relevant literature. Throughout the chapter, the presented approaches are well related to the goals of the thesis. In detail, Justyna Zawada first gives a brief overview of fault models and ATPG, before she explains the basic ideas of design for test (DFT) and scan-based test. Then she presents the standard STUMPS architecture for pseudo-random BIST using multiple scan chains, a linear feedback shift register (LFSR) for on-chip pattern generation and a multiple input signature register (MISR) for test response evaluation. Furthermore, she briefly discusses test data compression within the framework of

embedded test (EDT), where the ATPG patterns are stored in a compressed format in an external memory and regenerated on chip by suitable hardware blocks. Subsequently, she describes an example of hybrid BIST emphasizing that the reuse of the random pattern generator as a decompressor is an important prerequisite for the success of such a scheme. Finally, the last subsection is dedicated to security issues. Here, Justyna Zawada focuses on the protection against reverse engineering attacks and reviews previously published techniques based on logic blocking.

The following four chapters contain the new approaches for test point insertion developed within the framework of this thesis. Chapter 3 is devoted to conflict resolution in ATPG. Justina Zawada introduces the problem with the help of an instructive example. She characterizes a typical conflict in ATPG where the propagation of different fault sets requires complementary values on logic lines that fan out from the same stem. In such a situation, the faults can only be propagated at the same time, if control points are used. After a deeper analysis of fault blocking and propagation, Justina Zawada develops two metrics quantifying the conflict potential. The first metric is based on the number of zeros and ones needed to propagate all faults starting from a line x, and the second metric counts the number of zeros and ones obtained on line x by forward implication. The conflict potential is then assessed comparing the complementary instances of both metrics. The algorithm for test point insertion computes the metrics in one pass through the circuit and considers all fanout stems as candidates for control points. In each iteration, the algorithm selects the fanout stem with highest conflict potential, updates all metrics and reconsiders decisions from previous iterations. The algorithm stops when the budget of test points is used up. A comprehensive experimental study at the end of the chapter shows that the new conflict test points, which are also called EDT test points, can considerably reduce the ATPG pattern count. Further experiments include functional flip-flops as drivers of the control points. Here the results show, that EDT test points allow a very good trade-off between pattern count and test coverage. Moreover, they also help to reduce the ATPG run time.

In Chapter 4 the concept is extended to hyprid BIST. The work is motivated by experimental data showing that test point insertion targeting random pattern testability provides only limited support for conflict resolution in ATPG and vice versa. Again an instructive example highlights a typical “hybrid” conflict where the requirements for fault propagation at fanout branches are combined with a low signal probability of the desired value at the fanout stem. Thus, the conflict potential is characterized by combining the already developed metrics with COP-based controllability measures. The algorithm for hybrid test point insertion then proceeds iteratively similar as the algorithm for EDT test points. But here, test point insertion can also be controlled by a probabilistic estimation of the achieved test coverage. For this the known COP controllability and observability measures are extended, such that signal dependencies due to reconvergent fanout can be better approximated. As the experimental results show, testability analysis using the newly introduced weighted controllability and observability measures achieve a high accuracy much closer to exact fault simulation than the standard approach. The experimental study at the end of Chapter 4 also demonstrates that the concept of hybrid test points in fact successfully addresses both the random pattern testability and the ATPG requirements.

In Chapter 5 Justyna Zawada investigates a BIST scheme for in-field test, which efficiently combines a standard scan-based BIST with test-per-clock features. In this scheme, observation points are organized as additional enhanced scan chains supporting a per clock test response evaluation. The observation chains basically perform signature analysis enabled by integrated XOR gates. The scheme also deploys control points with their drivers residing in extra standard scan chains or interspersed

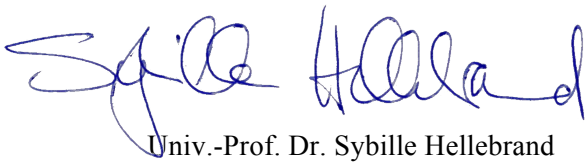
between regular scan cells. To support test point insertion for this scheme, Justina Zawada introduces the observation performance as an additional testability metric. The algorithm for test point insertion then again starts with testability analysis. However, in each iteration the algorithm now tries both the best option for a control and for an observation point, and the test point with the larger impact on test coverage is selected. An experimental study compares the new BIST approach with a conventional logic BIST. It can be observed, that for all examples the new scheme combined with a proper selection of test points can achieve the same test coverage in a significantly shorter test time.

Subsequently, Chapter 6 deals with the security threats introduced by the test infrastructure. The presented approach assumes a state-of-the art access protection, for example by a challenge response authentication using a physically unclonable function (PUF). Whenever an unauthorized access is detected, then the existing test points in the design are gradually activated to change the logic function. In the experimental evaluation the capability of obfuscating the functional logic is measured by the reachability of primary outputs and scan cells from control points. The respective problem of transitive closure is analyzed for several circuits, and it can be seen that in most cases a high percentage of primary outputs and scan cells is reached within a few clock cycles. In another experiment, Justyna Zawada uses random simulations to determine the perturbation introduced by control points. This experiment also shows that activating the hybrid test points in the design can quickly change a large percentage of primary outputs and scan cells. A short discussion of possible attacks completes the presented work on security aspects. Finally, Chapter 7 concludes the manuscript with a short review of the four developed techniques.

Overall, Justyna Zawada has developed very good solutions for a highly relevant research problem in different application scenarios. In addition to the conceptual work, she has validated the proposed approaches for test point insertion by experimental case studies targeting large industrial designs. Her work is based on a comprehensive yet concise review of the relevant literature and relies on appropriate strategies. As confirmed by the experimental analysis, the four strategies for test point insertion developed within the framework of the thesis support a high quality test throughout the life cycle of a system and allow for an excellent trade-off between pattern count and test coverage. Interestingly, the test points can also contribute to protecting the chip against reverse engineering. The achieved results are clearly ahead of the state of the art, which is also confirmed by a number of peer-reviewed publications in internationally recognized conferences and journals as well as by two US patent applications. Furthermore, due to the successful cooperation with Mentor Graphics Corp., the thesis is also very strong with respect to its practical applicability. The underlying assumptions are based on realistic industrial data, and the developed procedures can easily be integrated into an industrial design flow.

The manuscript provides a clear description of the developed approaches and gives the expert reader a complete picture of the work. For the non-expert reader, it would have been helpful to include a more self-contained description of the background and the state of the art. For example, a more detailed introduction into testability analysis as well as the discussion of a standard approach for test point insertion could have given a better starting point for the non-expert reader. Concerning the security aspects dealt with in Chapter 7, I would have appreciated more in-depth information how the effectiveness of logic blocking is evaluated in other state-of-the art approaches, and how the robustness against attacks is generally measured.

Despite these minor deficiencies, the thesis fulfills the requirements for the degree of Doctor of Philosophy as stated by the current law and its quality is clearly above the average. Therefore, I strongly recommend accepting thesis as submitted and rating it as “very good”.



Paderborn, August 15, 2017 Univ.-Prof. Dr. Sybille Hellebrand