Dr. Prof. Giorgio Di Natale
CNRS / Université Grenoble-Alpes – TIMA
46, avenue Félix Viallet
38031 Grenoble, France
giorgio.di-natale@univ-grenoble-alpes.fr

16/06/2024

Reviewer's opinion

on Ph.D. dissertation authored by

BARTOSZ WŁODARCZAK

entitled:

ON SECURE DETERMINISTIC IN-SYSTEM TEST SOLUTIONS

1. Problem and its impact

Most Important Problem Discussed:
The primary issue addressed in this thesis is the security and reliability of Deterministic In-System Test (DIST) solutions for Integrated Circuits (ICs). As ICs become more complex with billions of transistors, they face increased vulnerability to defects and security threats. This problem is highly relevant in domains such as automotive, data centers, and healthcare, where continuous and reliable testing throughout the product lifecycle is crucial to prevent malfunctions due to silicon degradation and other issues.

Scientific and Practical Relevance:
The problem is both scientific and practical. Scientifically, it deals with the challenge of enhancing IC test methods to handle large-scale data and unknown values (X states) while maintaining the integrity and security of the test infrastructure. Practically, it addresses the need for robust and secure ICs in critical applications, ensuring they remain operational and secure against unauthorized access and cyber threats. The thesis effectively identifies and tackles these critical challenges, making it a significant contribution to the field.

2. Contribution

Main Original Contribution:
The main contributions of the thesis are twofold:

1. **Advanced Test Response Compaction:** The development of new X-masking methods for test response compaction, specifically tailored for logic built-in self-test (BIST) environments and DIST scenarios. These methods enhance the ability to handle test data with unknown values and improve observability of scan errors without compromising test quality.
2. **Lightweight Cryptographic Schemes:** Introduction of novel lightweight cryptographic primitives, including a hybrid ring generator (HRG), a new cryptographic hash function, a stream cipher for test data, and a true random number generator. These contribute to forming a hardware root of trust that protects ICs against unauthorized access and other security threats.

Practicality of Proposed Solutions:
The proposed solutions are practical and address real-world challenges in IC testing and security. However, the review notes that certain aspects, such as the X-masking methods, could have been more thoroughly explained to enhance comprehension and practical applicability. Additionally, while the cryptographic schemes are well-conceived, a deeper exploration of their comparison with existing methods and their real-world deployment would strengthen the thesis (see Section 5 for more details)

3. Correctness

Overall, the claims made in the thesis are trustworthy and supported by rigorous analysis and experimental results. The proposed solutions are evaluated using comprehensive statistical tests and applied to large industrial designs, lending credibility to the findings.

Identified Shortcomings:

- Complexity of Explanation: Some sections, particularly those explaining the X-masking schemes, were challenging to understand due to the complexity and presentation style. This issue could have been mitigated by providing clearer diagrams and more concise explanations.
- Inadequate Definition: Certain terms, such as H2B in Section 7, are not clearly defined, which could confuse readers unfamiliar with the terminology.
- Side-Channel Analysis: The analysis of side-channel resistance is somewhat superficial, lacking detailed exploration of advanced attack methods and their implications for the proposed cryptographic primitives.
- Entropy Evaluation: The evaluation of entropy for the proposed true random number generator (TRNG) lacks formal proofs of the presence of good entropy.

Valued Aspects:

- Rigorous Statistical Testing: The thorough evaluation of cryptographic primitives using NIST and AIS-31 test suites is commendable.
- Comprehensive Analysis: The design and implementation of the test schemes are well-supported by experimental results, demonstrating a high level of technical competency.

4. Knowledge of the candidate

General Knowledge and Tutorial Quality:

- Chapter 2: Provides an overview of state-of-the-art X-masking solutions, demonstrating a solid understanding of the current landscape and laying the groundwork for the candidate's contributions.
- Chapters 5-10: Cover common security issues in IC testing, cryptographic hash functions, stream ciphers, and the development of lightweight cryptographic primitives. These sections showcase the candidate's in-depth knowledge in the discipline and their ability to apply this knowledge to practical problems.

Quality and Completeness:
The chapters are generally well-written and reflect a comprehensive understanding of the field. The references are extensive and relevant, though a more structured approach in certain sections would enhance clarity (see Section 5 for more details)

Opinion on List of References:
The list of references is complete and demonstrates thorough research.

Other Arguments:
The thesis exhibits a broad understanding of Information and Communication Technology (ICT), particularly in secure IC testing and cryptographic methods. The candidate's ability to integrate these areas into practical solutions for real-world challenges further supports their competence in the discipline.

5. Other remarks

- **Section 3:** The diagrams (e.g., Figure 3.1) would benefit from using standard symbols for common elements. For instance, Flip-flops (FFs) could be represented with rectangles that include the classic clock triangle symbol.
- **Section 7.1:** The phrase "The muxes select randomly and per-cycle data produced by HRG and its phase shifter" should be corrected to "pseudo-randomly," as the selection is determined by a complex, yet deterministic, function rather than true randomness.
- **Section 7.1:** The Algebraic Normal Form (ANF) format would be clearer if it used the XOR operator instead of the OR operator, which is correctly applied after equation 7.1.
- **Section 7.3 (Side-Channel Analysis):** This section provides a good initial approximation of the side-channel analysis. It would be beneficial to include power measurements or simulations. Additionally, consider the impact of electromagnetic (EM) probes, which can be placed on specific parts of the circuit.
- **Table 7.7:** For better comprehension, it would be preferable to group versions with the same parallelism (e.g., 128, 256, 512). The throughput values appear inconsistent, particularly in the last rows. The power metrics should be explained more thoroughly, as the text provides limited details. Showing power consumption per bit per second (bps) and energy per bit would be useful.
- **Section 8.1:** The statement "These ciphers must be very fast – they have to match the speed of SSN typically operating at much higher shift frequencies than in-core DFT logic does" requires clarification on the specific speed or frequency required.
- **Section 8.4:** The note about space constraints affecting the tables is inappropriate for a Ph.D. thesis, which should not be subject to such limitations. All relevant data should be included for thoroughness.
- **Table 8.1:** The meaning of the columns is unclear and needs further explanation or labeling to improve understanding.
- **Section 8.4:** The primary motivation mentioned is minimizing area overhead, but there is no comparison with existing, certified methods. Including such comparisons would strengthen the evaluation.
- **Section 8.5 (Algebraic Attacks):** The argument that non-linear operators can prevent algebraic attacks is insufficiently detailed. The thesis should discuss the level of non-linearity, how it can be measured, and how it compares to existing certified stream ciphers.
- **Section 8.5 (Side-Channel Resistance):** The claim that the design is resistant to side-channel attacks is not entirely accurate. Side-channel attacks typically use differential methods to remove noise. A more convincing proof would involve testing the solution against the latest

known attacks and measuring how many observations are needed to uncover the secret. Metrics like Side-Channel Vulnerability Factors could provide additional insights.

- **Proposed TRNG:** The entropy of the true random number generator is not evaluated formally. It's also challenging to distinguish between the raw entropy source and the deterministic parts of the circuit. Despite these issues, the concept is innovative and holds promise.

6. 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?

[X]	[ ]	[ ]	[ ]	[ ]
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

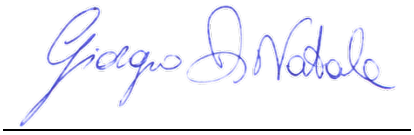
B. After reading the dissertation, would you agree that the candidate has general theoretical knowledge and understanding of the discipline of **Information and Communication Technology**, and particularly the area of **VLSI Testing and Hardware Security**?

[X]	[ ]	[ ]	[ ]	[ ]
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?

[X]	[ ]	[ ]	[ ]	[ ]
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

Overall, the thesis presents significant contributions to the field of IC testing and security. The proposed solutions are innovative and practical, addressing both theoretical and real-world challenges. I therefore **recommend to distinguish** the dissertation for its quality.



Signature

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