Prof. Dr. Mehdi Tahoori
Chair of Dependable Nano Computing
Karlsruhe Institute of Technology
76131 Karlsruhe, Germany
mehdi.tahoori@kit.edu

02.07.2024

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

BARTOSZ WŁODARCZAK

entitled:

ON SECURE DETERMINISTIC IN-SYSTEM TEST SOLUTIONS

1. Problem and its impact

Design for Test (DfT) infrastructure plays an important role in ensuring the quality of complex chips, with billions of transistors, fabricated in advanced technologies nodes, which are also used in safety critical domains such as automotive. To further improve the test quality, built-in self test (BIST) methods are integrated into the chip, enabling the chip itself to generate and apply test, as well as analysing the test responses. However, the security of test infrastructure particularly BIST and streaming scan remains a big challenge.

This dissertation explores the security challenges of the DfT infrastructure, in particular deterministic BIST, and provides scientific yet practical methods for securing the BIST infrastructure. The approaches presented in the dissertation have deep scientific foundation and at the same time significant practical relevance and impact. The research results have been published in the highest-rank international scientific journals and symposia.

2. Contribution

The dissertation contributes significantly to in-system test response compaction and lightweight cryptographic schemes for hardware security. It introduces two innovative X-masking methods designed for test response compaction in system tests. The first compactor is tailored for a logic built-in self-test environment, adept at managing test data from observation scan chains that can capture errors at each scan shift cycle. The second solution integrates tightly with a deterministic in-system test, receiving control signals from an on-chip test data decompressor. The design principles of selection logic and the rules for encoding masking data are thoroughly detailed.

In the area of lightweight cryptographic schemes, the dissertation proposes new methods to form a hardware root of trust, enhancing design IP protection and securing test infrastructure. It introduces a hybrid ring generator (HRG), a modified version of a conventional ring generator, which serves as the basis for three new cryptographic primitives: a cryptographic hash function, a stream cipher for test data, and a true random number generator. A hardware root of trust is developed based on these primitives to support challenge-response authentication protocols, featuring a low area footprint, high operational frequencies, and compatibility with design and DFT flow. While it primarily targets System-on-Chip

(SoC) solutions with packetized streaming of test data, it also enhances the security of other test interfaces.

The effectiveness of the proposed test response compactors has been validated through rigorous experimentation on large, complex industrial designs representing the latest technology nodes, covering various design styles and scan methodologies. The new security primitives have been verified using extensive statistical tests, including those provided by the National Institute of Standards and Technology (NIST) and the German IT security certification authority (BSI). These contributions advance the reliability of in-system testing and the security of hardware designs, offering practical solutions for modern electronic systems.

3. Correctness

The claims in the dissertation appear to be correct and trustworthy. I did not find particular scientific flaws in this work.

4. Knowledge of the candidate

The dissertation includes chapters (1-5) that serve as tutorials, confirming the candidate's general knowledge in Computing, particularly in built-in self-test, test compression, cryptography, and hardware security. These tutorial-like chapters cover areas such as the principles of X-masking methods for in-system test response compaction, the integration of deterministic in-system tests, and the design and encoding rules for masking data. Additionally, the sections on lightweight cryptographic schemes, including the hybrid ring generator, cryptographic hash functions, stream ciphers, and true random number generators, highlight a deep understanding of hardware security. The quality of these chapters is high, as they provide thorough explanations and detailed design principles, supported by extensive experimental validation and statistical testing. The references are comprehensive, citing relevant and authoritative sources, demonstrating the candidate's familiarity with current research and practices in Computing. These elements collectively argue strongly in favor of the candidate's broad and thorough understanding of the discipline.

5. Other remarks[1]

None

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)[2], 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**)

☒ □ □ □ □

[1] Optional

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

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*

M Tahoori

Signature