Development and Application of Embedded Test Instruments to Digital, Analog/RFs and Secure ICs

Florence Azaïs, Serge Bernard, Mariane Comte, Bastien Deveautour, Sophie Dupuis, Hassan El Badawi, Marie-Lise Flottes, Patrick Girard, Vincent Kerzérho, Laurent Latorre, et al.

Development and Application of Embedded Test Instruments to Digital, Analog/RFs and Secure ICs

F. Azaïs[1], S. Bernard[1], M. Comte[1], B. Deveautour[1], S. Dupuis[1], H. El Badawi[1], M.-L. Flottes[1], P. Girard[1], V. Kerzerho[1], L. Latorre[1], F. Lefèvre[2], B. Rouzeyre[1], E. Valea[1], T. Vayssade[1], A. Virazel[1]

[1] LIRMM, Univ. of Montpellier / CNRS – Montpellier, France
<lastname>@lirmm.fr

[2] NXP Semiconductors – Caen, France
francois.lefevre@nxp.com

***Abstract*— Systems on a chip have seen their surface area increased by a factor of 10 and their consumption multiplied by 5 during the last ten years. Each technological node that enabled this integration has also added new constraints challenging the overall system reliability. In addition, the integration of analog/RF blocks adds specific issues, in particular the high cost of the required test equipment. It is therefore necessary to improve test and reliability solutions in order to guarantee the production yield and the system life-time. Moreover, the massive increase in the use of communicating systems has introduced security as a cornerstone of their development. The entire hardware production flow is therefore subject to security and trust issues requiring the development of dedicated test solutions. In this paper, we focus on LIRMM contributions in the HADES project especially with details on Embedded Test Instruments (ETIs) for reliability of digital ICs, low-cost RF test based on indirect DC measurements or digital ATE capture, management of secure scan access.**

Keywords*— *ETI, Fault tolerance, AxC, RF testing, Machine Learning, Security and test, scan encryption.

I. Embedded Test Instruments for reliability of digital ICs

AxC (Approximate Computing) is an emerging computation paradigm in which an inaccurate result rather than a guaranteed accurate one can be accepted at the cost of a reduced accuracy [1]. AxC has already been explored for fault tolerance architecture. In [2] [3], the authors presented the Approximate Triple Modular Redundancy (ATMR) and its extension as Full ATMR. Authors in [4] show the interest of AxC for fault tolerance in arithmetic units by proposing a configurable-accuracy approximated adder.

In the framework of the HADES project, we exploit the AxC paradigm to build ETIs (Embedded Test Instruments) to improve the reliability of digital ICs. We have first analyzed the interest of using AxC circuits to build a duplication scheme. Secondly, we propose a fully robust approximation-based solution suitable for safety-critical applications that can reduce the cost compared to conventional TMR structures.

A. AxC-based duplication scheme for error detection in arithmetic circuits

An error detection architecture must be capable of detecting transient, permanent and timing faults that may occur in a arithmetic circuit. The error detection scheme we evaluate employs duplication and comparison to detect faults. Since the architecture relies on duplication of the arithmetic block and the use of a comparator, its implementation incurs an overhead of more than 100% in terms of area and power.

The different duplication scenarios we have considered:

- Scenario 1 (S1) – Full duplication scheme
- Scenario 2 (S2) – Reduced duplication scheme based on the structural susceptibility analysis [5]
- Scenario 3 (S3) – Reduced duplication scheme based on the logical weight
- Scenario 4 (S4) – Reduced duplication scheme based on an approximate structure

The four duplication scenarios are compared using arithmetic circuits. To compare the different scenarios (S1, S2, S3 and S4), we present the results achieved in terms of area and power consumption overhead with respect to S1, as well as EP (Error Probability) and WCE (Worst-Case Error) metric values.

Fig. 1 reports the comparisons of all scenarios with respect to S1 for an 8-bit adder. The different approximate version of the 8-bit adder have been taken form the open library available from a public benchmark suite [6]. These comparisons show that the use of an *AxC* circuit as reduced copy to build a duplication scheme seems to be a good alternative to build an error detection scheme for arithmetic circuits. In fact, this duplication scenario (*S4*) offers better values in terms of area and power overhead while reducing drastically the error metrics (i.e., *EP* and *WCE*) compared to the more conventional *S2* and *S3* duplication scenarios.

B. QAMR: Quadruple Approximate Modular Redundancy

The Quadruple Approximate Modular Redundancy (QAMR) is a novel scheme to ensure a full logic masking (tolerance) of transient and permanent faults. Like TMR, QAMR masks all faults occurring in the modules and for which the voter still has a majority of correct responses. It achieves the same accuracy than the TMR while still benefiting from approximation advantages (i.e., smaller area and power overhead). To implement the QAMR, we use four approximate circuit replicas. The fundamental condition to respect is that, at a given time, at least three precise responses (i.e., non-approximated) must be delivered by the QAMR structure. In other words, the four AxC ICs must be approximated in a complementary manner. This is obtained with an iterative

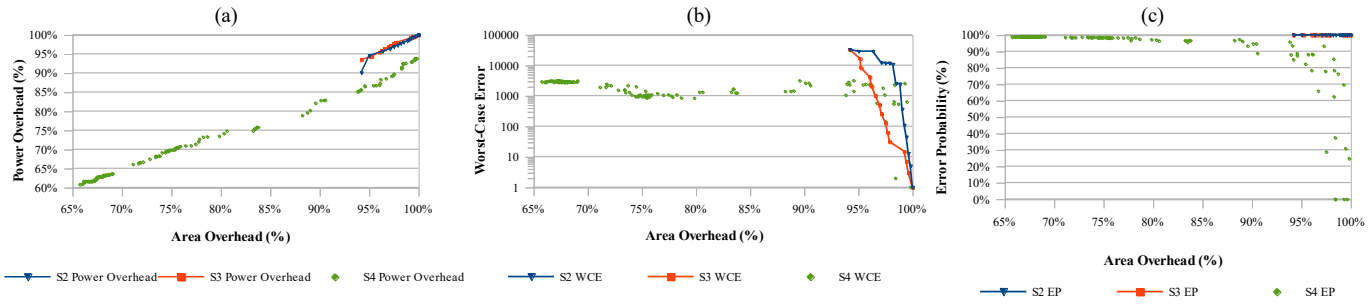

Fig. 1: Comparisons of all scenarios with respect to S1 for a 8-bits adder with a) Power overhead, b) WCE and c EP metrics

synthesis flow that generates multiple AxC ICs versions.

To compare our results with those obtained with the TMR scheme, we use a Relative Area Gain (RAG) metric. This means that we consider the TMR as our baseline with 0% of area gain. Thus, the higher the RAG, the better the QAMR area performance with respect to the TMR.

Fig. 2 shows results obtained ranked from circuits with the highest SLR (Shared Logic Rate) to circuits with the lowest. The SLR is the proportion of logic shared by more than one output logic cone. We observe that below 20% of SLR, our QAMR scheme underperforms the TMR most of the time. We can see that only 6 out of 23 circuits with an SLR lower than 20% have a positive RAG. On the other hand, 13 out of the 29 circuits with an SLR higher than 20% outperform the TMR versions by achieving a positive RAG. Those results confirm the interest of the presented design exploration.

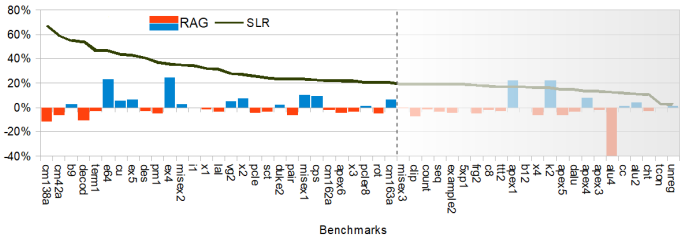

Fig. 2: Area gained by QAMR compared with TMR ordered by SLR

II. Low-cost solutions for production test of RF ICs

The cost of test is a major concern for most of the actors in the semiconductor market, especially for RF devices which are today embedded in many products via SoC or SiP technique and used in an increasing number of applications [7]. The current industrial practice relies on the use of an ATE equipped with specific analog/RF test instruments in order to measure the device performances. These resources are extremely expensive and constitute a dominant factor in the production testing costs. An interesting approach is to relax the constraints on the required test equipment by developing alternative solutions that can be implemented using only low-cost test resources. It is the objective of the work developed in the HADES project, with two different strategies described in the following sections.

A. Indirect test based on DC measurements and machine-learning algorithms

A first strategy is to develop an indirect test solution based on low-cost DC measurements (delivered by ETIs) and machine-learning algorithms. The idea is to implement an initial training phase in which machine-learning algorithms are used to establish the correlation between the DC measurements and the conventional analog/RF performance measurements. During the production testing phase, the performances of every new device are then evaluated based solely on the DC measurements using the regression models learned during the initial training phase. This strategy has been largely studied in the literature, focusing on different aspects such as definition of pertinent indirect measurements, choice of the machine-learning algorithm, composition of the learning set or insertion of a safety mechanism to improve prediction confidence. For each one of these aspects, many different solutions are possible; a comprehensive review of works can be found in [8].

Our work concerns the development of a generic framework that permits to explore the various options related to all these aspects. It includes a library of processing algorithms dedicated to data preparation, model exploration, model selection and test efficiency evaluation. It offers the possibility to build different types of models, either classical ones such as Multi-Linear Regression (MLR), Multi-Adaptive Regression Spline (MARS) or Support Vector Machine (SVM) models or ensemble models based on bagging, boosting or stacking [9]. It also offers the possibility to combine indirect test and standard specification test in a two-tier adaptive test flow in order to tradeoff test quality and test cost [10]. This framework constitutes an essential element to guide the test engineer in its choices for an efficient indirect test implementation.

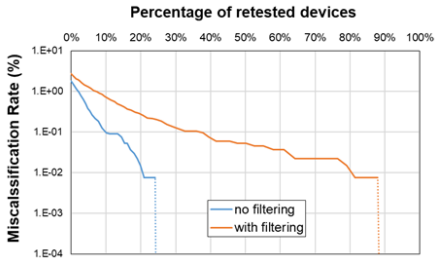

Fig. 3: Example of cost/efficiency tradeoff on WLAN frond-end RF IC

An example of the use of this framework for a front-end RF WLAN IC currently under development is shown in Fig.3. This figure reports the cost/efficiency tradeoff curves that can be obtained with a two-tier adaptive test flow. This figure shows that the use of a filter in the initial learning phase is not a pertinent choice. It also shows that substantial test cost reduction can be achieved without compromising test quality,

i.e., a misclassification rate below 0.1% with only 10% of devices that need to go through a standard specification test, and a perfect misclassification rate of 0% with less than 25% of the devices that need to go through a standard specification test.

B. *Indirect test based on 1-bit acquisition with standard digital ATE channel*

The second strategy relies on a direct acquisition of the RF signal to be analyzed with a standard digital ATE channel. Indeed, as illustrated in Fig. 4, a digital tester channel comprises a comparator and a latch that implement level-crossing with sampling. During this operation, the amplitude, frequency and/or phase information contained in the RF signal is converted in timing information into the resulting bitstream. The idea is then to develop dedicated post-processing algorithms able to retrieve this information and extract the main signal characteristics.

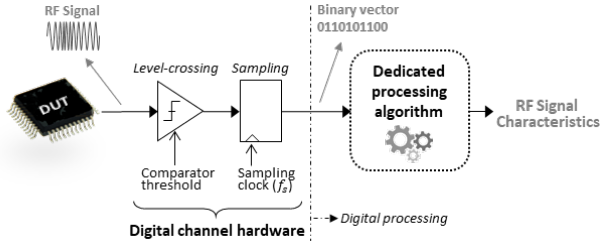

Fig. 4: Basic principle of the proposed approach

Our work focuses on the implementation of this strategy for a ZigBee Transceiver (2.4GHz signal modulated with OQPSK format and half-sine pulse shaping). The developed solution relies on 1-bit under-sampled acquisition of the RF signal with a sampling frequency close to half the carrier frequency in order to comply with the maximum sampling rate of standard digital channel (typically 1.6Gbps). This under-sampling process produces a digital signal with a fundamental beat frequency at a much lower range (few tens of MHz), but that still contains relevant information about the original RF signal. Dedicated software procedures have been developed that permit to extract both amplitude and phase fluctuations and therefore allow the reconstruction of the RF signal. Further procedures have then been developed to retrieve the symbol sequence present in the RF signal [11] and perform performance measurements on the reconstructed signal, such as power level measurements and spectral power spectrum evaluation [12].

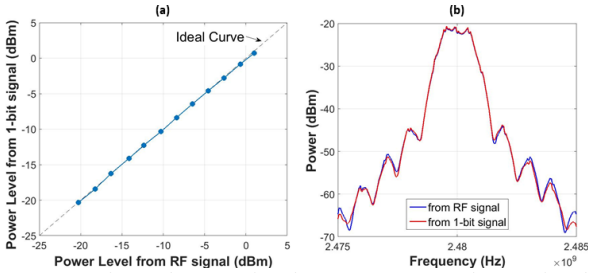

Fig. 5: Comparison of conventional measurement on the RF signal and estimation from 1-bit capture: (a) power level and (b) power spectrum

The proposed solution has been validated through hardware measurements realized both with an experimental lab setup and with an industrial ATE (Advantest V93k). An example of results is shown in Fig. 5 regarding power level measurements and power spectrum evaluation. In both cases, a good agreement is obtained between values measured on the RF signal and the ones computed from the 1-bit capture.

III. Secure Scan Access Management

DfT techniques make lean and effective testing practices possible throughout the entire product life cycle, but they also offer an unwanted security backdoor. For this reason, there is a need to design test infrastructures using a security-aware approach [13]. Many existing techniques use cryptographic implementations to prevent unauthorized access, or to provide confidentiality and integrity to test data transmitted between the user and the device. Among all the existing countermeasures, one of the most promising is the *scan encryption*. This countermeasure is based on the encryption of test data, which guarantees their confidentiality and prevents unauthorized use of the test infrastructure.

A. *Scan Encryption*

Scan encryption techniques have known a relatively recent development due to their promising characteristics. From a security perspective, they rely on data encryption based on symmetric ciphers. Encrypted test patterns are on-chip decrypted before application, while test responses are on-chip encrypted before transmission. Symmetric ciphers can be easily employed to set up a secure test flow. In fact, the test process can be seen as a communication between a tester and a device. The tester can be an authorized user accessing the test infrastructure in-the-field, or an ATE performing post-manufacturing test. The target device can be an integrated circuit, or a specific IP core inside a System-on-Chip (SoC) that has its internal test infrastructure protected. The designer chooses a secret key that is stored inside the device. Subsequently, this key must be handed out to all the parties that are authorized to access the test interface of the device [14]. The scan encryption technique merges both user authentication and data confidentiality into a unique security countermeasure. Any malicious device or malicious user trying to "sniff" the test channel in order to retrieve confidential data from the device under test faces encrypted and thus unintelligible message. Moreover, an unauthorized user that does not know the secret key it is not able to successfully encrypt input test data for proper activation/control of his/her target.For this reason, the only way to successfully communicate with the target device is to know the secret key and to properly encrypt all data that is introduced through the scan-in pin. Scan encryption schemes can be implemented using *block* or *stream* ciphers.

A block cipher encrypts *n*-bit blocks from a plaintext message and generates corresponding *n*-bit blocks ciphertext. The encryption process takes a fixed number of clock cycles. The same key is used for all the encryptions performed along the life cycle of the device. Lightweight block ciphers are preferred for the encryption of test infrastructures due to their reduced implementation cost. An example of lightweight block cipher that has been used for test data encryption is the PRESENT block cipher [14].

A stream cipher performs a bit-wise XOR operation between the plaintext and a pseudo-random bit stream, called *keystream*. The keystream is generated by a pseudo-random generator, which is the core of the stream cipher. The TRIVIUM stream cipher has been experimented in this context due to its lightweight hardware implementation. In the TRIVIUM stream cipher the keystream generation is initialized by an 80-bit secret key and an 80-bit Initialization Vector (IV). While the key must be secret and constant, the IV is a never-repeating value that is publicly known. The first requirement that must be fulfilled in order to consider a stream cipher secure is the generation of an unpredictable keystream so that it is impossible to retrieve the plaintext from the ciphertext without knowing the keystream. The second requirement is to never use the same keystream more than once, in order to prevent *two-times pad attacks* [15][16].

B. Which Scan Encryption is Better?

We evaluate stream-based and block-based test data encryption schemes according to different cost and qualityfactors: area/power consumption/test time overheads and security level.

A PRESENT block cipher and a TRIVIUM stream cipher have similar costs in terms of area and power consumption. However, implementation on current complex devices leads to different costs. The block-based solution requires two ciphers: one for decryption of input test data, the other for encryption of test responses. Conversely, the stream-based solution requires only one stream cipher for generation of both decryption and encryption keystreams (encryption and decryption being implemented by simple XOR operations). Therefore, the block-based solution implies twice the area and power overhead compared to the stream-based approach.

Concerning the TRIVIUM stream cipher, an additional initialization test time of 1152 clock cycles is required , representing a marginal test time overhead compared to the millions of clock cycles needed to test a complex device of billions of transistors. Moreover, since both the test infrastructure and the stream cipher have a serial interface, no additional timing overhead is required. On the other hand, the parallel interface of the block cipher requires padding test data into a multiple of the block size. The padding of test data results in additional clock cycles, implying a test time overhead on each test vector. This results in a higher test time overhead than stream-based solutions. Alternative solutions using extra observation points for both test pattern length optimization and efficient data padding allows to lower test time impact of block-based approaches.

Table 1. Comparison Overview

Cost Function	Stream Cipher	Block Cipher
Area	+	-
Power	+	-
Test Time	+	-
Security	-	+

From the security point of view, stream-based solutions from previous related literature are vulnerable to *two-times pad attacks*. An attacker has indeed the possibility to force the generation of the same keystream to encrypt more than one plaintext. This security flaw is not present in block-based solutions Table 1 summarizes pros and cons of both approaches. We proposed a proper management of both secret key and IV for security improvement of the stream-based encrypted test scheme.

ACKNOWLEDGMENT

This work has been carried out under the framework of PENTA project “HADES: Hierarchy-Aware and secure embedded test infrastructure for Dependability and performance Enhancement of integrated Systems”.

REFERENCES

[1] Q. Xu, et al., “Approximate computing: A survey,” IEEE Design Test, vol. 33, no. 1, pp. 8–22, Feb 2016.

[2] I. A.C. Gomes, et al. “Exploring the use of approximate TMR to mask transient faults in logic with low area overhead,” Microelectronics Reliability, vol 55, no 9–10, 2015, pp. 2072-2076.

[3] A. J. Sanchez-Clemente, et al., "Error Mitigation Using Approximate Logic Circuits : A Comparison of Probabilistic and Evolutionary Approaches," IEEE Transactions on Reliability, vol. 65, no. 4, pp. 1871-1883, Dec. 2016.

[4] K. Al-Maaitah, I. Qiqieh, A.Soltan, A. Yakovlev, “Configurable-accuracy approximate adder design with light-weight fast convergence error recovery circuit,” IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), 2017, pp. 1-6.

[5] I. Wali, et al., “A Low-Cost Reliability vs. Cost Trade-Off Methodology to Selectively Harden Logic Circuits,” Journal of Electronic Testing – Theory and Applications, vol. 33, no. 31, pp. 25–36, February 2017.

[6] V. Mrazek, et al., “Evoapprox8b: Library of Approx Adders and Multipliers for Circuit Design and Benchmarking of Approximation Methods,” in Proc. of IEEE/ACM/EDAA Design Automation and Test in Europe, 2017, pp. 258–261.

[7] F. Demmerle, "Integrated RF-CMOS Transceivers challenge RF Test," Proc. IEEE International Test Conference (ITC), 2006.

[8] H. Stratigopoulos, “Machine learning applications in IC testing”, Proc. IEEE European Test Symposium (ETS), pp.1-10, 2018.

[9] H. El Badawi et al., "Investigations on the Use of Ensemble Methods for Specification-Oriented Indirect Test of RF Circuits", Journal of Electronics Testing, 2020.

[10] H. El Badawi et al., "Implementing indirect test of RF circuits without compromising test quality: a practical case study", Proc. IEEE Latin-American Test Symposium (LATS), pp.1-6, 2020.

[11] T. Vayssade et al., “Low-cost functional test of a 2.4 GHz OQPSK transmitter using standard digital ATE”, Proc. IEEE Int’l On-Line Test Conferance (IOLTS), pp.1-.6, 2018.

[12] T. Vayssade et al., “Power measurement and spectral test of ZigBee transmitters from 1-bit under-sampled acquisition”, Proc. IEEE European Test Symposium (ETS), pp.1-6, 2019.

[13] E. Valea, M. Da Silva, G. Di Natale, M. Flottes and B. Rouzeyre, "A Survey on Security Threats and Countermeasures in IEEE Test Standards," in IEEE Design & Test, vol. 36, no. 3, pp. 95-116, June 2019, doi: 10.1109/MDAT.2019.2899064.

[14] M. Da Silva, et al., “Preventing Scan Attacks on Secure Circuits Through Scan Chain Encryption,” IEEE TCAD 2018.

[15] M. Da Silva, E. Valea, M. l. Flottes, S. Dupuis, G. Di Natale and B. Rouzeyre, “A new secure stream cipher for scan chain encryption,” In IVSW 2018.

[16] E. Valea, M. Da Silva, M.-L. Flottes, G. Di Natale, B. Rouzeyre, “Stream vs block ciphers for scan encryption”, Microelectronics Journal, Volume 86, 2019, Pages 65-76.