A NOVEL ACCESS SCHEME FOR ONLINE TEST IN RFID MEMORIES

Prathap[1], Ramesh[2], Rajeshwari Soma[3]
[1]M. Tech (VLSI), [2]Assoc. Prof. (ECE)
Ganapathy Engg. College, Rangasaipet, Warangal, A.P., India
[3]M. Tech (VLSI), JITS, Narsampet, Warangal, A.P., India

ABSTRACT
Radio Frequency Identification (RFID) devices depend on the correct operation of their memory for guaranteeing accurate identification and delivery of transponder's information. In this paper, a novel approach for online testing of RFIDs based on March-BIST techniques for EEPROMs is resented. Online test is achieved by modifying the transponder's operation and access protocol to exploit the waiting time that transponders waste before being accessed. The solution was described in VHDL, simulated and synthesized to obtain area and timing results. Results show that the solution overhead is less than 0.1 %, while the timing performance allows testing up to 32-word blocks in a single waiting slot

1. INTRODUCTION

Radio Frequency Identification (RFID) devices are the main constituting actors in the Internet of Things paradigm, where they are used to face the challenge of labeling physical objects to allow them to participate in the digital world. Such RFID devices rely on their memory to accomplish their function which range from the simple read-only transponder to the high end transponder with intelligent crypto logical modules. Read-only transponders represent the low-end, low-cost segment of the range of RFID data carriers. As soon as such transponder enters the interrogation zone of a reader, a scheme to access its identification number is deployed. The tag's unique identification number is hardwired into the transponder during chip manufacture; therefore, the user cannot alter this serial number, or any data on the chip. Writable transponders can be written by the interrogator and their memory may have several kilobits. Write and read access to the transponder is often performed in blocks of, usually, 16 bits, as in the EPC Class 1 Generation 2 protocol (C1G2). Recent developments aim at increasing RFID data rate to 10 Mbps, which entails the possibility of incrementing memory capacity to 1 Mbyte or more. Considering the trend to increase memory capacity in RFIDs, a new RFID architecture and access scheme is proposed that allows concurrent online tests of the transponder memory. A built-in self-test (BIST) controller with appropriate march-tests is carefully exploited to check for memory errors. The following of this paper is organized as follows. In Section II, the general operation of the transponder and the typical organization of its memory are presented. Section III describes the regular accessing scheme of the transponder and the modifications proposed to allow the online test of the memory. In Section IV and V a description of the March algorithms utilized is shown and the BIST architecture is introduced. Section VI provides the simulation and synthesis results while in Section VII conclusions and future work are drawn.

2. TANSPONDER OPERATION

Following a top-down approach, the transponder protocols are defined in three different layers: application, communication and physical. In the application layer, the transponder receives commands from the interrogator that are valid only when the tag has been singled out. These commands generally consist of writing, reading or locking the tag's internal memory. At this layer, an

interrogator may be able to terminate indefinitely the tag's operation by issuing a password-protected command. The communication layer allows an interrogator to manage tag populations while embracing an anti-collision protocol. A great number of tags may be controlled by supervising tag's data collisions. A regular scheme to avoid collisions employs a two-part scheme where an interrogator, first, selects a broad number of tags and, subsequently, forces them to randomly choose access slots. This access mechanism is employed within the EPC C1G2 protocol and is based in the Dynamic Framed Slotted ALOHA algorithm (DFSA) [4]. To support access from several interrogators, transponders provide session flags that may be asserted or de asserted by interrogators. Session flags allow interrogators to organize groups of tags and force them to enter a particular inventory round. Transponder memory is organized in agreement with different standards, but, commonly, it follows a division in banks according to the function of the memory portion as follows: Reserved memory, which includes passwords for accessing special tag functions. Product Identification memory, which is a code used to identify the object containing the tag. Tag Identifier memory, which is the unique identification number of the tag. User memory, which is an application specific bank.

3. TEST-ORIENTED ACCESS SCHEME

The normal operation of an interrogator, when accessing a set of transponders, relies on subsequent selections of smaller groups of tags and random assignment of access slots. This selection procedure is time-consuming and does not involve reading or writing the memory for transponders that are in the interrogator queue. A selection command issued by the interrogator impels a tag or group of tags to set or unset their internal flags according to a comparison mask. In this way, an interrogator is able to split in smallest sets a larger group of tags in order to access them easily. Typically, an interrogator starts a new inventory pointing towards a previously selected set of tags. Transponders matching the interrogator's flags selection must generate an internal random Queue Position Number (QPN) which represents its assigned slot in the DFSA algorithm. The maximum QPN available for the transponders is determined by the interrogator each time an inventory starts. In order to establish a direct link interrogator-transponder, the interrogator sends a command which is answered only by transponders which QPN is equal to zero. Meanwhile, the other transponders involved in the inventory should decrement their own QPN by one, until their turn to answer the interrogator comes. The success of the anti-collision scheme relies in the effectiveness of the interrogator to select an appropriate maximum value for the QPN which avoids picking the same time slot by more than one transponder. Every transponder is accessed individually while the others remain in an Arbitrate state waiting for their access slot. In the Arbitrate state, transponders are fully powered by the interrogator signal but no particular operation is being executed. The concurrent online access scheme proposed exploits this waiting state to perform the test of the memory and is based on the anti-collision mechanism of EPC C1G2 standard.

A. Selection Stage

Every transponder works in one of four sessions and has separate inventoried flag for each. These flags determine whether the transponder may respond to the interrogator or not within an inventory round. A Selected flag (SL) also exists which purpose is to ensure a greater accuracy during management of large transponder populations. The proposed scheme introduces a Test flag which can be asserted by the interrogator to force transponders to a testing state while being accessed. An interrogator issues a Select command to select a particular transponder population by asserting or de asserting their flags. This command aims at a particular flag and forces its value, e.g., a SL flag is asserted. Within the proposed scheme, the interrogator chooses the population of tags to be tested by asserting its Test flag with the Select command.

B. Testing Stage

Fig. 1 shows the proposed finite state machine (FSM) of the transponder access scheme. Once a transponder is within the range of an interrogator, it reaches the Ready state. The Ready

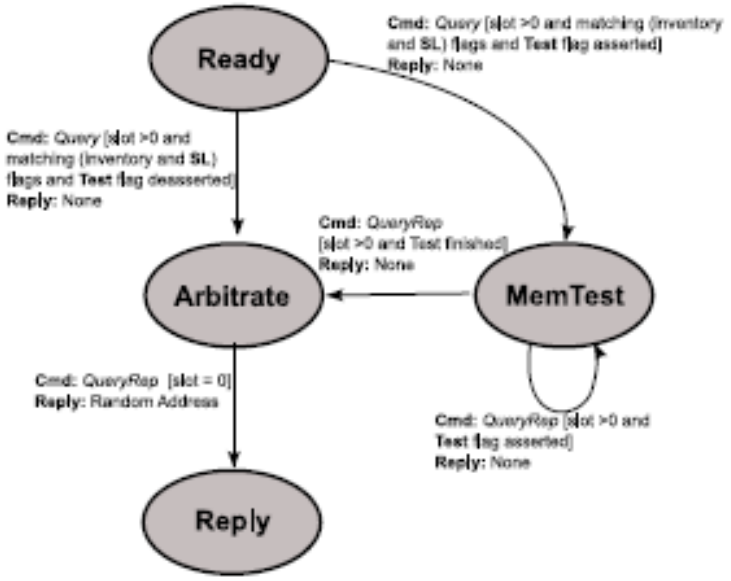

Fig.1 Transponder access scheme with concurrent test state

State is a holding state for energized transponders that are not participating in an inventory round. A transponder that is in Ready state accepts Select commands from the interrogator that force it to set or unset session flags. The transition from the Ready to the Arbitrate state is done when the interrogator broadcasts a Query command with a session flag as a parameter. Transponders matching the session flag transit to Arbitrate, the others stay in Ready and do not participate in the inventory round. Every transponder, ti, going to Arbitrate chooses randomly a QPNi. The access scheme allows the interrogator to adaptively choose an adequate interval of QPN in order to consider the number of transponders available in the inventory round or the time needed to finish the memory test. Consequently, by issuing commands to transponders, the interrogator forces them to pass from Arbitrate to Ready back and forward until the QPN interval is appropriate for the current inventory round. QPN_i's valid values are defined as: $QPN_i 2 [0; 2^Q-1]$; with Q being chosen by the interrogator for each inventory round. Regular operation of the interrogator-transponders interaction consists of command-based transitions from the Arbitrate state to the Reply state by transponders which QPN is equal to zero. The interrogator has full access to the transponder and its memory within the Reply state. The proposed testing approach includes a new state for testing, Mem Test, which sends a signal to a BIST controller to start the test of a given memory block and keeps track of its result. To prevent unwanted behavior, a transponder t_i in the Mem Test state reacts only to the Query Rep command which forces the decrement of QPN_i, i.e., changes to the next time slot. An extra 32-bit register is implemented in the transponder to be used as a memory block counter during the test process. The information regarding the memory block to test is sent through data lines towards the BIST. A transponder within Ready state which receives a Query command with matching flags, and with the test flag asserted, should go to Mem Test state and should compute its QPN. In this case, QPN should be selected to allow the whole test of the memory, thus, the QPN value randomly chosen within the regular interval is increased by a fixed offset equal to the number of memory blocks to test. Concurrently, the memory block counter is loaded with the number of the first memory block. When the test is finished, the transponder transits to the Arbitrate state to continue with the regular operation related to accessing its information. In order to inform the interrogator that an error has been detected, the transponder should transit to the Reply state while sending a temporary random identifier accompanied with an error code. The error code describes the nature of the error and the place where it has been detected as well. In case of no error detection or while in regular operation, the transponder should backscatter only the temporary identifier.

4. MARCH TEST ALGORITHM

Many algorithms have been developed for testing semiconductor memories, from which the most popular and advantageous are the March tests. A March test contains a sequence of March elements

which is composed by a read/write operation that has to be performed into every cell of the memory. March tests are able to detect several fault models such as Stuck-at Faults (SAF), Address Faults (AF) and some Coupling Faults (CF). The operations that can be executed in the cells may be: write zero (w0), write one (w1), read zero (r0) and read one (r1). The read operation checks if the value inside the cell is the expected one. The order in which cells are considered can be ascending or descending. A typical march test used to test RAMs is MATS++ which can be adapted to test also EEPROMs. The MATS++ algorithm is described as follows:
l (w0); " (r0;w1); # (r1;w0; r0):
Word-oriented memories, such the ones found in an RFID, need a slightly different approach. By extending the 0 or 1 to 16 bits, march algorithm can be easily applied to RFID's word-oriented memories with a reduction on the coverage of CF.

A. Symmetric Transparent Test

Regular march tests produce the erase of the contents in the memory. To prevent losing data a transparent approach is introduced. The transparent method avoids traditional comparison and, instead, uses a signature analysis mechanism based on a feedback shift register. Well-known march tests can be easily extended to transparent versions by replacing values 0 and 1, in the read and write operations, by a and ac, respectively, where a refers to original content and ac to its complement. Besides this modification, the initialization part in the original march test should be removed. A symmetric transparent test poses a constraint on the symmetry of the March test, e.g., it should have the same number of reading for the original and the complement content, since the signature mechanism computes the signature when fed by the original content and computes the reciprocal signature when fed by the complementary content. By doing so, the initial state of the signature mechanism should be found at the end of the test when the memory is fault free.

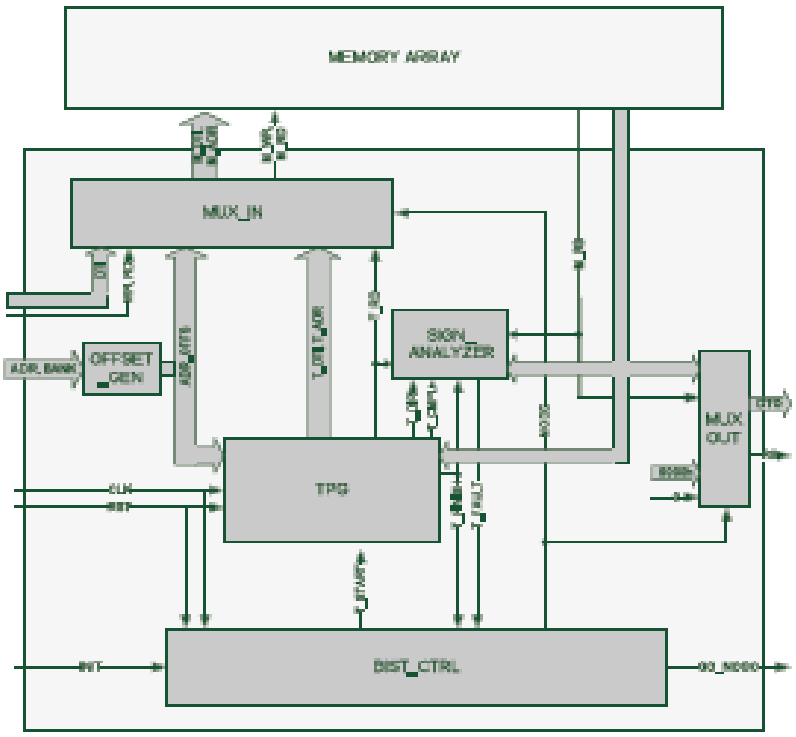

Fig 2. Architecture of the memory module with BIST controller

5. MEMORY BIST IMPLEMENTATION

Figure 2 shows the architecture of the BIST module composed by six entities: offset generator, memory input multiplexer, output multiplexer, BIST controller, signature analyzer and test pattern generator. The function of the input multiplexer is to choose which signals input to the memory according to the BIST mode. The output multiplexer provides constant values and the ready/busy (RB) signal is set to zero throughout all the test period. The offset generator is a module that modifies

incoming address depending on the bank selected for the memory during regular operation. The BIST controller captures the init signal from the transponder's FSM and starts the test procedure. The test pattern generator is responsible for generating the test vectors to be introduced to the memory. It contains the sequence and directions of the march test in a configuration array. Its implementation consists of a FSM which takes information from the configuration array and performs their instructions, while the complement of the data read from the memory is used as input when needed. The signature analyzer is a Multiple Input Shift Register (MISR) with a flow signal that sets its direction of propagation. This implementation avoids the use of two different shift registers for the signature and the reciprocal signature computation. To reduce the probability of error masking, an irreducible polynomial was selected for the MISR; it has the following form:
$H(x) = 1 + x^7 + x^9 + x^{12} + x^{16}$:
Additional methods to avoid error masking involves hardware solutions, e.g., additional check parity, the use of hamming codes or larger MISRs, which are undesirable for the constrained RFID system due their overhead.

6. SIMULATION AND EVALUATION

The proposed scheme was synthesized and simulated in order to evaluate its performance regarding timing and area

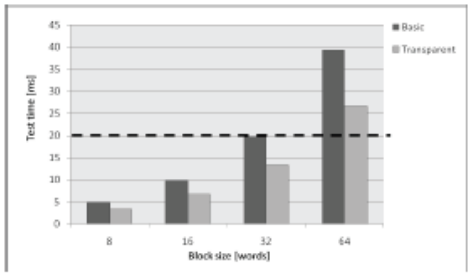

Fig 3. Test time for transparent and basic MATS++

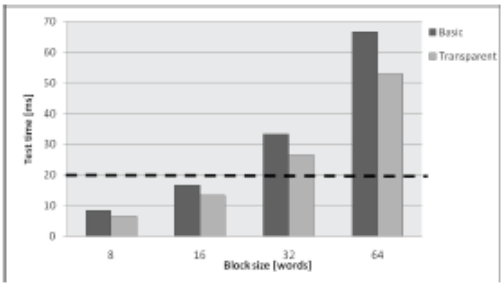

Fig 4. Test time for transparent and basic MARCHC

TABLE – I
BIST AREA OVERHEAD

Technology	Memory Area	BIST Area	Overhead
0.65 μm	9.7 mm^2	0.0094 mm^2	0.1%

Overhead. The BIST scheme was described in VHDL and synthesized using a 0.65m technology. The BIST used the transponder's internal clock signal which is obtained from the interrogator carrier frequency, and was chosen equal to 1 MHz the evaluation of the area overhead was calculated considering the memory since it is the largest component of the transponder. A memory capacity of 1 kB was assumed, which is, in average, larger than the capacity of most of current passive transponders. The area overhead was computed as AO = BIST Area Memory Area _ 100%. To obtain realistic values for the memory area, the data was extrapolated from. The results related to the

memory overhead are shown, for this particular case, in Table I. Passive transponders are equipped with a capacitor charged by the electromagnetic field generated by the interrogator. Continuous read and write operations during the test causes high current consumption, hence a charge in the capacitor can rapidly fall down. As an example, circuit presented in contains a 250 pF capacitor which stores energy supplies during short gaps in the received signal for about 100 _s. In such time, it is possible to perform some read operations, but writing could be interrupted. Thus, testing of a single memory block should be as short as possible to decrease the risk of that situation. As a safe threshold, the time of the longest operation specified by the EPC C1G2 standard was assumed as the limit for the testing operation of a memory block in the RFID, i.e., 20 ms. to evaluate the timing performance of the circuit two March tests were executed: the MATS++ algorithm, described before, and the March C- algorithm. The March C- algorithm has a higher complexity than MATS++ and is described in the following in its transparent version:
"(rac);"(ra;wac);"(rac;wa);#(ra;wac);#(rac;wa);#(ra):
Figure 3 and 4 present the results of the simulation in terms of timing for the MATS++ and March C- algorithms respectively. The simulations were performed varying the testing block sizes. Furthermore, the timing information of the basic approach is also presented to compare with the transparent approach. The 20 ms threshold is also highlighted for convenience. As can be seen in the simulations results, the absence of the initialization stage in the transparent approach provides an interesting reduction of test time. In average, the time is reduced by 32 % for MATS++ and by 20.5 % for the MarchC algorithm. These simulations show the maximum block size which can be tested within one single slot according to the algorithm utilized. For the MATS++ algorithm, the maximum testing block size is 32 words, while for the March C- the maximum is 16 words.

7. CONCLUSIONS AND FUTURE WORK

A novel access scheme supporting online test for RFIDs was presented. The novel schemes take advantages of the idle state of transponders while waiting to be accessed by the interrogator to perform the test of their internal memory. The transponder finite state machine describing the access scheme was presented and the architecture of the transparent BIST circuit was described. Synthesis and simulation results show the feasibility of the proposed scheme. Area results show the negligible overhead of the BIST in terms of area compared with the memory size, i.e., about 0.1 %. Timing results present the maximum size of blocks that can be tested within one slot of the accessing scheme by considering two different march algorithms. Future work will include other testing approaches which provide a direct testing command to the interrogator and a larger list of supported march algorithms.

REFERENCES

[1] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using rfid: The rfid ecosystem experience," Internet Computing, IEEE, vol. 13, no. 3, pp. 48–55, may-june 2009.
[2] EPCGlobal, EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID air interface Version 1.2.0, Oct. 2008.
[3] J. McDonnell, J. Waters, H. Balinsky, R. Castle, F. Dickin, W. W. Loh, and K. Shepherd, "Memory spot: A labeling technology," Pervasive Computing, IEEE, vol. 9, no. 2, pp. 11–17, april-june 2010
[4] T. Cheng and L. Jin, "Analysis and simulation of rfid anti-collision algorithms," in Advanced Communication Technology, The 9th International Conference on, vol. 1, 2007, pp. 697–701.
[5] M. L. Bushnell and V. D. Agrawal, Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits. Springer, 2000.
[6] S. Hellebrand, H.-J. Wunderlich, and V. Yarmolik, "Symmetric transparent bist for rams," Design, Automation and Test in Europe Conference and Exhibition, vol. 0, p. 702, 1999.
[7] D. R. Banerjee, S; Chowdhury, "Built-in self-test for flash memory embedded in soc," in Third IEEE International Workshop on Electronic Design, Test and Applications, DELTA 2006., January 2006.
[8] U. Karthaus and M. Fischer, "Fully integrated passive uhf rfid transponder ic with 16.7- mu;w minimum rf input power," Solid-State Circuits, IEEE Journal of, vol. 38, no. 10, pp. 1602 – 1608, 2003