Abstract

This thesis reports a study of a class of non-group cellular automata (CA), namely TPSA (two predecessors and single attractor) CA for both its analysis & synthesis and its application for hash function generation and message authentication. Further we have established the application of CA for recursive pseudo–exhaustive pattern generation for built-in-self-test environment. For testing of synchronous sequential circuits, we have again advocated a CA based scheme, which with some associated circuitry has been shown to compact data up to 95% over direct storage for benchmark circuits.

We have done theoretical studies on the properties of a class of non-group CA called TPSA CA with a matrix theoretic approach. We have presented an algorithm for generating a class of TPSA CA with 90 and 150 rules. Further we have developed a general method of constructing TPSA CA using all possible additive rules; lower bound of the total number of such TPSA CA that can be constructed is $2^n - 1$ where n is the length of CA. The issue of *general* hashing and the collision free *perfect* hashing for a given key set, has been taken up. We have studied the case of TPSA CA as an efficient hashing function generator for both perfect and general hashing. The quality of the proposed scheme is competitive to division method from the view point of collision and expected overflow. ASIC design of a TPSA CA based comparatively cheaper associative memory employing the combined strategy of rehashing and chaining is also presented. A message authentication scheme, derived from the state transition behaviour of TPSA CA, has been proposed in this thesis. It is significantly different from conventional approaches. The proposed scheme is superior in terms of CPU time (50% reduction) for software implementation compared to standard MD-5 algorithm, the most commonly used method. The CA based hardware can achieve further speed improvement approximately by at least three order. Regular, modular, and cascadable structure of CA with local interconnections makes the scheme

ideally suitable for VLSI implementation. The design has been specified in Verilog, simulated for functional correctness, and synthesized using the tool Synergy from Cadence. For complex circuits with large number of inputs, pseudo exhaustive testing has been found to be suitable for many cases where each of the outputs depends only on a subset of the inputs. This results in much smaller test size compared to the exhaustive test size of 2^n for n-input circuit under test (CUT). We have presented a recursive technique for generation of pseudo exhaustive test patterns. The scheme is optimal in the sense that first 2^k vectors cover all adjacent k-bit spaces exhaustively. The scheme has been proved to generate recursive pseudo-exhaustive test pattern using CA employing 204 and 106 rules for built-in-self-test (BIST) applications. It has been shown analytically that hardware cost reduction by the proposed scheme is up to 50% as compared to the previously reported methods. Testing of sequential circuits is more involved because to test a particular stuck-at-fault, the test patterns are to be applied in a specified sequence only. This may introduce a number of idle cycles between two successive test patterns, thus increasing the test application time. We have shown that CA with some associated circuitry can produce on–chip specified sequence of test patterns without incorporation of idle cycles. The results for benchmark circuits show an improvement of up to 95% over direct memory storage.

KEYWORDS: Cellular Automata (CA), Characteristic matrix, Non-group CA, Group CA, Complemented CA, Recursive pseudo-exhaustive testing, Hash function, Re–hashing, Message authentication, Digital signature, Automatic test sequence generator (ATSG), Data compaction.