Chapter 3

LITERATURE SURVEY

3.1 Scope of the Previous Work

This Chapter surveys the previous work reported in literature on test vector compression and security of testing process. As design sizes have grown larger and semiconductor manufacturing processes have scaled down to extremely small feature sizes, the number of test vectors needed to thoroughly test a chip have exploded. To alleviate this potentially road-blocking issue, test data compression became an active research topic in the late 1990s. It has now become a standard solution within commercial DFT tools. State-of-the-art compression schemes can achieve 10x to 100x reduction in both tester cycles and data volume. This might sound incredible, considering that Moore’s law has been predicting only about 2x reduction every 12 to 18 months. High density of manufacturing faults are popping up as the technology is entering its saturation in complementary metal oxide semiconductor (CMOS) and exploring new avenues beyond CMOS. Beyond CMOS refers to emerging research devices, focussing on a new switch used to process information, typically exploiting a new state variable to provide functional scaling substantially beyond that attainable by ultimately scaled CMOS. It is defined in terms of functional density, increased
performance, dramatically reduced power, etc. The different avenues of technologies beyond CMOS are shown in Figure 3.1.

![Figure 3.1: Computing and data storage beyond CMOS (ITRS, 2008)](image)

### 3.2 State-of-the-Art Methods on Test Data Compression

In the past, several researchers have investigated the feasibility of replacing the ATPG with BIST by making suitable modifications in the BIST techniques to achieve comparable fault coverage with ATPG. Early work on LFSR designs for random patterns based testing was performed. A design technique for linear feedback shift registers that generate test patterns for pseudo-exhaustive testing is presented (Wang and McCluskey, 1986). This technique is applicable to any combinational network in which none of the outputs depends on all inputs. It does not rewire the original network inputs during in-circuit test pattern generation. Thus, the possibility of undetected faults on some inputs is eliminated. This technique mostly
discusses methods for worst case circuits and there are other methods that generally result in test sets of smaller size.

A core with a virtual scan chain reduces test costs for the system integrator (Abhijit, et al., 2004). Thus, core vendors may find virtual scan chains as a means to achieve a competitive advantage. But in this work, the default ordering of the scan chains was used. It was assumed that the core designer would want to choose the ordering of the scan chain based on other criteria such as minimizing routing. However, one way to improve the results would be to specially order the scan chain. The scan cells could be partitioned into scan sub chains in a way that equally distributes the specified bits in the test cubes in order to minimize the size of the LFSRs and/or maximize the amount of static compaction that can be performed.

Two methods for improving the compression of linear compression schemes, scan inversion, and reconfiguration of the de-compressor, have been proposed (Balakrishnan, 2006). A systematic procedure based on linear algebra was described for selecting the set of inverted scan cells. Simulation results show that scan inversion can dramatically improve the encoding efficiency of combinational linear decompressors bringing it close to that of sequential decompressors. Scan inversion can be implemented with no hardware overhead. The reconfiguration of a linear decompressor is represented as a constrained Boolean matrix and a symbolic Gaussian elimination method is proposed to solve it. Reconfiguration requires very little extra hardware. Experimental results show that compression obtained using a linear decompressor can be significantly improved using reconfiguration.

A deterministic BIST method that combines test-generation, LFSR-seed encod-
ing and fault simulation to achieve high fault coverage as deterministic ATPG has been attempted (Peter, et al., 2003). The number of patterns encoded into a single LFSR seed varies continuously to accommodate the most efficient encoding. LFSR seeds control all care bits in all patterns. It also presented a mechanism that allows seeds to be loaded and the LFSR reseeded with no cycle overhead. The resulting patterns are fully compatible with scan testers. DBIST can be applied to all fault models that deterministic test generation supports. DBIST can also be implemented as self contained BIST, storing the seeds on-chip. Both test data volume and tester cycles are significantly reduced over highly compacted deterministic patterns while obtaining the same test coverage. The method presented is fully integrated into an automated flow that performs all design modifications, rules checking and DBIST pattern generation.

A seed-ordering technique based on the transition matrix of the PRPG and efficiently exploiting the don’t care bits in the test patterns is presented (Ahmad, et al., 2005). The simulation experiments showed that the number of seeds required for 100% stuck at fault coverage is reduced by up to 80% when this ordering technique is used compared to arbitrary ordering. This technique avoids high complexity like previous analytical solutions and avoids long simulation times. A scheme for representing a seed by the number of PRPG cycles required to reach it is also presented. The simulation experiments showed that the storage needed is reduced by 25%-85% when this encoding technique is used compared to storing a single seed per pattern. The main characteristics that made this techniques effective are: 1) exploiting the linearity of the LFSR and the associativity of matrix multiplication
to avoid simulation 2) avoiding unnecessary computation to reduce the complexity of ordering the seeds 3) exploiting the don’t cares in test patterns and 4) applying pseudorandom patterns intelligently between deterministic patterns to reduce the number of seeds required to be loaded. However this method needs to be combined with ATPG to produce high fault coverage.

A method of reversing the test vector order from end of the list and analyzing the trend of fault coverage is explained (Hochbaum, 1996). The problem of optimal test compression is to derive, from a given set of test vectors, a smallest possible subset of test vectors that still test for the same collection of faults. This achieves optimal compression and largest reduction possible in test time relative to the original set of test vectors. Approach based on the modeling of the problem as the set cover problem was used. Additionally, the approach implies an ordering of the faults according to the difficulty of covering them with the given set of test vectors. As such it can be used to facilitate the finding of a solution to the ultimate smallest test-set, the compression of the set of all possible test vectors. It highlights the potential usefulness of integer programming techniques in testing and design. The running time of the linear programming relaxation procedure, is low enough to merit its incorporation as a final phase to follow any test generation and compression procedure. The ordering of the test vectors make little impact on the fault coverage in random pattern testing. The impact on the fault coverage in random pattern testing varies with different designs.

In (Tobias, 2012), a single cycle access structure is discussed. Various implementations with and without hold mode as well as gated and partial implementation
methods are presented. The aspects feasibility, peak power consumption, switching activity during test, area, test cycles, at-speed testing and debugging features are compared. A guide decision is given how to select the best implementation. The best solution gSCAS (gated single cycle access structure) is compared to RAS (random access scan) implementations and is superior to all known RAS solutions. If BIST is preferable due to limited chip inputs and outputs or partial scan implementation, an address controlled BIST is discussed. The ATPG algorithms can be enhanced with the same methods SS (shift scan) implementations are optimized. Future work is related to algorithms for reducing the test cycles per net itself, register reordering, pattern optimization for activity reduction and de-compression methods for BIST using the gSCAS.

(Kenichi, et al., 2003) proposed a technique for selecting the LFSR seeds used in VLSI BISTs, for a given primitive polynomial, to improve test quality. It focuses on decreasing test length and increasing the number of detected faults. First, this work presented an algorithm for a test-per-clock BIST from which a seed was derived that has a minimum test length to cover the target fault. This work also presented an algorithm for a test-per-scan BIST from which a seed was derived that detected the maximum number of faults with a fixed test length. This technique was applied to the ISCAS'85 benchmark circuits and combinational parts of the ISCAS'89 benchmark circuits. The fewer undetected faults remaining, the fewer additional circuits required. Thus, the proposed seed selection algorithms can be applied not only to conventional BISTs but also mixed-mode BISTs such as those with reseeding, bit-flipping, and bit-fixing. This method does not consider the ATPG test vectors to
find the minimum test length.

(Wang, et al., 1987) demonstrated to design a \((p, y)\) LFSR in such a way that it is an \(p\) stage autonomous LFSR of period \(2^y - 1\) such that \(y < p\). The problem of exhaustive testing of the \((n, w)\) CUT is to obtain the smallest integer \(y\) such that any \(w\) combinations of the \((p, y)\) LFSR outputs contain all \(2^w\) distinct test patterns (states) where \(w \leq y < n\). Theorem 1 in Wang’s method shows that the \((p, y)\) LFSR, with the smallest integer \(y\) is capable of exhaustively testing the CUT provided the following two conditions are met. 1) The characteristic polynomial of the LFSR is of the form:

\[
f(x) = g(x).p(x) = (1 + x + x^2 + \ldots + x^{n-y}).p(x)
\]  

where \(p(x)\) is a primitive polynomial of degree \(k\) and \(g(x)\) is any monic polynomial of degree \(n-k\).

A low-power test pattern generation method that could be easily implemented by hardware was proposed (Feng Liang, et al., 2013). It also developed a theory to express a sequence generated by linear sequential architectures, and extracted a class of single input change (SIC) sequences named multiple SIC (MSIC). Analysis results showed that an MSIC sequence had the favorable features of uniform distribution, low input transition density, and low dependency relationship between the test length and the TPG’s initial states. Combined with the proposed reconfigurable Johnson counter or scalable SIC counter, the MSIC-TPG can be easily implemented, and is flexible to test-per-clock schemes and test-per-scan schemes. For a test-per-clock scheme, the MSIC-TPG applies SIC sequences to the CUT with the SRAM-like grid. For a test-per-scan scheme, the MSIC-TPG converts an SIC
vector to low transition vectors for all scan chains. Implementation results and analysis results demonstrate that the MSIC-TPG is scalable to scan length, and has small impact on the test overhead.

(Shabaz, 2015) proposed a reconfigurable 2D LFSR to generate test patterns for BIST used in SoC embedded cores. It generates test patterns in a more pseudo-random manner and hence increases the fault coverage of the design. It contains a configuration network (CN), Control unit(CU), Multiplexer and Demultiplexer block and a flip-flop array. This method is useful for testing SoC with a large numbers of cores within it. This technique reduces the hardware architecture for testing multiple cores.

(Zacharia, et al., 1995) proposes a new and very efficient scheme to decompress deterministic test vectors, to be used as part of a built-in test strategy using mixed-mode pattern generation. The scheme is based on the reseeding of an multiple polynomial LFSR (MP-LFSR) and exploits variable-length seeds to encode the deterministic test vectors. The required hardware is very simple and introduces some area overhead. It shares the LFSR used for pseudorandom test vector generation and some scan flip-flops (Figure 3.2). The method is compatible with scan designs and relies on mature automatic test pattern generation techniques to produce the test cubes. The scheme is also compatible with any fault models as long as the test cubes can be obtained. The overall scheme, when used as a part of mixed-mode testing, offers many attractive trade-offs in terms of test data and test application time to achieve complete fault coverage. Moreover, it offers reduced bandwidth requirements as all the data transfers involve compressed data. The hardware decompressor
is well integrated with STUMPS designs. Furthermore, since the seeds are loaded serially, the approach is compatible with low-pin-count testers and boundary scan architecture. In the latter case, the entire decompressor structure is viewed as the user defined test data registers accessible through the boundary scan interface. The proposed schemes can be used in conjunction with test point insertion and offer many attractive trade-offs between test data storage and test application time to achieve complete fault coverage. Whereas all the experiments were done with single stuck-at fault model, the scheme is compatible with any fault model as long as the deterministic test cubes can be generated and produces small overhead in area.

![Diagram of decompression using variable length seed LFSRs](image)

Figure 3.2: Decompression of test data using variable length seed LFSRs (Zacharia, 1995)

(Tsai, 2000) demonstrated that the scan-based BIST architecture with full scan, may not result in the highest fault coverage (FC) and unscanning a small number of scan flip-flops may increase the BIST FC. It presents an algorithm for identifying those not-to-be-scanned flip-flops. It also shows that the general scan-based BIST test application scheme could also result in higher BIST FC and requires a minor modification to the BIST controller.

A synthesis procedure for generating sequence altering logic to embed deterministic test cubes in a pseudorandom sequence has been presented (Touba and
McCluskey, 2001). It constructs a sequential multilevel circuit that very efficiently encodes the deterministic test cubes. This approach can achieve any desired fault coverage during BIST by detecting the random pattern resistant (r.p.r.) faults missed by the pseudorandom patterns. There are three important features of the mixed-mode scheme presented in this method. The first is that test cubes for the r.p.r. faults are embedded in the pseudorandom bit sequence. Since there are so many possible pseudorandom patterns in which to embed each test cube, the bit fixing required to embed a set of test cubes can be correlated in certain bit positions to minimize hardware. The second feature is that a one-phase test is used. Having only one phase simplifies the BIST control logic. The third feature is that smaller LFSRs can be used. There is a tradeoff between the size of the LFSR and the amount of bit-fixing logic, therefore, the LFSR size can be chosen to minimize the overall area. These three features make the scheme presented in this paper an attractive option for BIST in circuits with scan.

(Anshuman and Krishnendu, 2002) have addressed the problems of test data volume and power consumption for scan vectors for system-on-a-chip testing. Since static compaction of scan vectors invariably leads to higher power for scan testing, the conflicting goals of low-power scan testing and reduced test data volume appear to be irreconcilable. This method employed test data compression to tackle these problems. This approach allows to reduce test data volume and scan power simultaneously. In particular, this method shown that Golomb coding of precomputed test sets leads to significant savings in peak and average power, without requiring either a slower scan clock or blocking logic in the scan cells. Further improvement is shown
on Golomb coding by showing that a separate cyclical scan register is not necessary for pattern decompression. Results for the larger ISCAS’89 benchmarks and for an IBM production circuit show that reduced test data volume and low-power scan testing can indeed be achieved in all cases.

(Rajski, et al., 2004) the embedded deterministic test (EDT) method tries to reduce manufacturing test cost by providing a reduction in scan test data volume and scan test time. The EDT logic can be placed either as a wrapper surrounding the original design, or it can be instantiated within the design. In both cases, however, it does not affect the functional paths. Given a design, the architecture of the EDT logic depends primarily on the number of internal scan chains, the number of external channels, the number of specified positions and a target compression ratio, as well as the number of captured unknown states. In particular, the decompressor size is usually chosen as a small multiplicity of the number of test pins, large enough, however, to maintain high encoding efficiency. Only logic that lies at the interface of the EDT hardware and the scan chains depends on the clocking of the first and last scan cells in every scan chain. The EDT logic is therefore pattern independent and in most cases does not have to be regenerated if a design changes.

3.3 Security Issues in Testing

JTAG is a widely used IEEE 1149.1 compatible test and debug standard interface for chip, board and systems. A JTAG consists of built in terminals which includes a serial input test data input (TDI), a serial output test data output (TDO), a test clock (TCK) and a control input test mode select (TMS). It also includes an optional
terminal called test reset (TRST) (IEEE 1149.1, 2001) (Parker, 2002). TMS controls the movement between 16 states of the TAP controller. JTAG is a test interface for the accessing the circuit’s internal logic. Initially JTAG was considered without security features. Technology growth results in many side-channels that can be threat to the devices. JTAG port is widely prone to this type of side-channel attacks (Tehranipoor, 2012). Logic BIST is initialized, enabled and disabled through JTAG. So it is necessary to provide security not only to the JTAG but also to the logic BIST. Several solutions were being proposed for securing JTAG during debugging and testing. Some of the previous protection methods are explained below. To the best of our knowledge, no protection mechanisms were suggested/applied to logic BIST till date in the literature.

Logic BIST is emerging as the second most widely used DFT techniques in the VLSI industry next to Boundary scan. JTAG refers to a standard Test Access Port (TAP) and boundary scan architecture. JTAG port act as the interaction point between the external world and the devices and it also provides access to the internal components for the purpose of circuit debug and configuration. In JTAG, testing and debugging is carried through one of the main hardware component Test Access Port. It is a static, digital interconnection test. JTAG is used to solve many of the testability problems in the today’s higher density devices. A TAP/JTAG controller is a module that controls and co-ordinates the operations of the entire test architecture. In recent years, the process of testing ICs result in many security problems such as side-channel attacks. Confidential data and IP of a device can be breached through standard DFT techniques. One of the main sources of side-channel attack is the
insecure JTAG port. Thus test structures can leak information about the chip design. BIST is an alternate solution for reducing the security risk associated with the testability. Cryptographic properties (Stallings, 2007) can be efficiently used to implement BIST techniques. Some existing works related to testing techniques and their security measures are explained in the following sections.

### 3.4 Previous Work on Security of IC Testing

(Baang, 1993) proposed an architecture for JTAG boundary-scan interface controller. It is implemented as a basic RISC (reduced instruction set computing) microprocessor. Techniques of code compression and pipeline simplify the data path and control logic. The way in which Interface Controller is designed and implemented makes its application more flexible. It supports many kinds of hardware assemble projection. For making the interface user friendly, a JTAG test language is also presented here. Test language simplifies the design of test programs. (Lavo, 2000) proposed an architecture for IEEE 1149.1 standard test access port with reusing capability. This is done by defining core architecture from the basic elements of the 1149.1 standard and applying a few simple designs guidelines during the RTL design of the TAP controller. This provides significant benefits for both TAP developers and users. This methodology will improve both design and support productivity, as well as provide a model for other areas of design reuse. Core architecture of the Open TAP controller is shown in Figure 3.3.

(Kahng, et al., 2001) proposed a method based on watermarking principles to protect Intellectual Property (IP) of the digital design. Watermark design is an
invisible identification code which is permanently embedded as an integral part of the design that supports design reuse. Watermark addresses IP protection by tracing unauthorized reuse and making untraceable unauthorized reuse as difficult as recreating given pieces of IP from scratch. This scheme imposes stronger constraints so that the watermarked IPs must remain functionally correct. Constraints can be achieved by using pre/post-processing of inputs and outputs respectively for a given design optimization. Moreover, this approach is compatible with current IP development tools and can be applied to protect both hardware IP and software IP.

(Koushanfar, F. and Gang, Qu., 2001) proposed a hardware metering scheme that enables the designers to securely control licensing rights for their IPs. The key idea is to make a very small part of the design programmable at the configuration time and to consequently configure this part for each manufactured chip in a unique way. Different configurations correspond to differently scheduled implementations or
have different register assignments. The advantage of this hardware scheme is that it has lower hardware overhead. It also provides some levels of protection against reverse engineering. Ability of the scheme to implement large number of chips each with different ID is also demonstrated here.

(Mitra, McCluskey and Makar, 2002) proposed a technique for designing and testing the TAP controller which is also used for some non-testing purposes such as loading configuration bits in FPGA, controlling the logic BIST circuits, etc. Here TAP controller is designed and tested using CED (Concurrent Error Detection) technique and this technique does not require any extra I/O pins. A very short test sequence is used to exhaustively test TAP controller design and this makes the testing of TAP controllers extremely simple. This technique performs self testing during system operation for special purposes.

(Gassend, et al., 2002) describe about Controlled Physical Random Function (CPRF). CPRFs are PRFs that can only be accessed via an algorithm that is physically bound to the PRF in an inseparable way. It is used to establish a shared secret with a specific physical device and it is flexible enough to allow multiple mutually mistrusting parties to securely use the same device. This can be used in various authenticated identification applications. CPRFs can also be used to ensure that a piece of code only runs on a processor chip that has a specific identity defined by a PRF (i.e Certified execution). It has some benefits, like protection against malicious nodes in distributed computation networks.

(Ronald and Barbara, 2006) discussed about a protected JTAG that controls protection level of the device and hence limits the acceptable interaction that takes
place through JTAG port during different phase of product development. The core characteristics of this architecture are hardware implementation, diverse levels of access, and a highly secure mechanism based on the generation of challenge/response pair for each access and hence can be used by a wide variety of users and safe from security threat. Debug and test operations are performed during the implementation phase. It complements a trusted platform, offering important debugging features and yet protecting secure information. Figure 3.4 shows the block diagram of protected JTAG and its environment. It consists of four functional components: Protected JTAG Interface, Access Manager, Level Controller and Modified JTAG port. (Whetsel, 2006) proposed a JTAG interface with high speed, reduced pin count

![Figure 3.4: Protected JTAG architecture (Ronald and Barbara, 2006)](image)

that can be used in all digital ICs which cannot implement a full JTAG test interface. This interface offers high speed full duplex communication over a single wire
using SBT (simultaneously bi-directional transceiver) technology. Interface can operate in either point-to-point configuration to support high speed applications or in a multi-drop configuration to support JTAG boundary scan applications. Operation of this interface is transparent to JTAG test patterns. Figure 3.5 shows the reduced pin count JTAG interface and controller. (Akselrod, 2008) presented and analyzed debug port controller architectures for SoC integrated circuits. JTAG based test and debug structures in the modern SoC has wide variety of functions such as Observability and controllability of the I/O ports of the ICs, providing security against various side-channels, power management, clocking scheme management, etc. Figure 3.6 shows the top level tap controller with and without some of the core IP tap controllers.

(Jian-min, 2009) proposed a functional enhancement methodology to standard IEEE 1149.1 JTAG controller by analyzing the chip architecture and debug schemes.
In addition to the traditional boundary scan tests enhanced features of the extended JTAG controller also performs test functions such as stuck-at scan, at-speed scan, memory BIST, on-chip real-time debug features etc.

(Zhao, Xiao and Han, 2009) proposed a scheme that applies boundary scan technology to FPGA based systems. This scheme uses the internal boundary scan testing circuits of the target FPGA system. Two steps involved in the FPGA based systems are configure and verify. Configuration is the process of loading a design programming file into FPGA and verification is the process of testing the function of FPGA. Boundary scan controller is designed in VHDL. It is simple, stable, reliable, all-purpose and avoids resource waste.

(Rosenfeld and Karri, 2010) analyzed various possible JTAG attacks and proposed protection scheme. Security problems arise when there is a discrepancy be-
tween what people expect and what assurances a given system can provide. It presents different ways in which an attacker can exploit a JTAG interface, different capabilities of attacker, and its countermeasures. Five JTAG (with daisy chain topology) based attacks were discussed in this paper. They are sniff secret data, read-out secret, test vector collection attack, modify state of authentic part, return false responses to the test. It presents a security scheme with three standard security primitives: a hash function, stream cipher (trivium) and MAC (Message Authentication Code) that significantly enhance the security of the device. This protection scheme provides significant improvement in JTAG security with reasonable costs and it is flexible as it can provide high assurance for important chips and low assurance for less important chips. Figure 3.7 shows the different kinds of attacks and defense capabilities. But in this scheme, the service server i.e. the device is trusted and thereby performing one way authentication. However, encryption has to be provided for the data to protect it from the attackers. Sometimes the chips in the same board cannot be trusted.

(Park, et al., 2010) proposed a credentials based security system for JTAG test structure shown in Figure 3.8. Here each device relies on credentials provided by a server and passwords to authenticate users and control user access to JTAG ports. Components of the mechanism are the authentication server for issuing credentials. Secure JTAG hardware for user verification and access control, and the host for relaying communication between the server and the user. The security of the communication between components is guaranteed by the authentication protocol. Hash and XOR calculations are employed in its authentication protocol. Since this
Figure 3.7: Conceptual security model (Rosenfeld and Karri, 2010)

approach is independent of application environment, it is easily applicable to all standards JTAG environment. The tradeoff for security is the area overhead of adding the hash crypto modules.

(Rosenfeld and Karri, 2011) proposed a security enhancement scheme for SoC test access. It prevents untrustworthy cores from sniffing data available on the test bus. This approach maintains economy of shared wiring while achieving security benefits of star topology test access wiring. It reduces the risk of cascading security failure in the subsystem modules. The scheme establishes distinct cryptographic session key with each of the cores and without any hard-coded secrets in the design. Here SoC integrator uses its control over the inter-core wiring to maintain the security of the test data. Area overhead and test time overhead is very small. SoC
Figure 3.8: Architecture of secure JTAG (Park, et al., 2010)

is a heterogeneous mixture of a number of cores (modules) collected from different vendors and embedded in a single IC. Hence, limiting the damage done by a single distinct core has become an important concern with a practical solution.

(Hely, Kurt Rosenfeld and Ramesh Karri, 2011) describes about various security issues associated with the VLSI testing and some countermeasures. High test coverage is very essential for the security because production flaws could induce new faults that result in the malfunctioning of the product. They also mentioned about the main parameters which characterize a secure DFT technique. It includes

- Test coverage and test penalty
- Compatibility with tools, design penalty
• Resistance against protocol attack

• Resistance against brute-force attack

It also mentioned some countermeasures to mitigate test related security hazards. They deal with test protocol, scan-chain design and test pattern generation. Some countermeasures are protocol level, scan chain-level protection, communication security for test channel, pattern watermarking. One approach of protection includes differentiation of user mode from the test mode and it is widely adopted by the SoC type designs. This research also mentions that in terms of security there is no universal protection possible. (Pierce and Tragoudas, 2011) proposed a multilevel privilege security system for JTAG controller. It monitors and controls the individual scan chain and hence restricts the malicious data being loaded into the JTAG controller. Multi-level privilege system allows for in the field updates, and debugging of the firmware while maintaining a high degree of protection for the most sensitive intellectual property in the IC. As shown in Figure 3.9, this security system consists of two primary components: security authentication module (SAM) and Access Monitor (AM). This security mechanism minimizes the risk of broad distribution of keys by restricting common keys to lower permission levels. The hardware additions of the proposed scheme are complaint with IEEE 1149.1 standard and requires no modifications to the FSM of JTAG controller. The security approach also assumed the design as trusted party. Therefore it is possible for fake circuits to obtain proprietary updates. Also this approach ends in considerable area overhead.

(Pooja, et al., 2012) proposed a multilevel security mechanism for the JTAG
architecture and prevent unauthorized users from accessing the private and confidential information of the device. This security scheme provides various privileges to different users that determine the area they can access based on their authorization. Privilege levels will be decided by the designer of the IC. Various privilege level offered includes P1, P2, P3 and P4. This scheme consists of an authentication and authorization module and an access provider mechanism. It uses advanced encryption standard (AES) Encryption/Decryption for private key generation and Challenge-Response protocol for authorization. Proposed architecture is fully compatible with IEEE 1149.1 standard and requires no modification to the JTAG TAP controller. But this approach also ends up in considerable area, power and speed overhead to the test structure.
(Yoo, Park and Kim, 2012) described about a real-life complete software solution for a JTAG security system. This solution provides benefits such as ease of use/administration, complete functionality, scalability, maintainability, and practicality. This method consists of three components Secure JTAG, the Host Computer, and the Secure Authentication Server. Secure JTAG is a hardware module that allows blocking and unblocking of the JTAG functionality through user authentication, the Host Computer is the computer of JTAG user where the JTAG tests are performed, and the Authentication Server is the secure component where the user account information of JTAG users is stored. As shown in Figure 3.10, this method is a system level software based password protected solution. In this scheme, only those users who own the correct credential issued by the Server and its password are allowed to use the JTAG port.

![Figure 3.10: Architectural model (Yoo, Park and Kim, 2012)](image-url)
(Das, et al., 2013) proposed and secure JTAG using ECC (Elliptical Curve Cryptography) based schnorr test protocol. This scheme uses Public Key Cryptography (PKC) protocol to solve the inherent key management problem. Zero-knowledge property of the schnorr protocol ensures the privacy of the authenticating devices. This makes use of certificates instead of shared symmetric keys. It consists of ECC based schnorr controller and ECC point multiplier that has been integrated with the JTAG interface along with other modules. Block diagram of proposed secure JTAG architecture with schnorr protocol is shown in Figure 3.11. It presents a mechanism for mutual authentication between the secure device and the tester. It does not make any modification to the existing JTAG interface. But PKC is more hardware expensive and slower than SKC (Symmetric Key Cryptography).

(Pierce and Tragoudas, 2013) proposed an enhanced secure architecture for the JTAG. The security mechanism monitors each scan chain and can restrict which

![Figure 3.11: JTAG ECC controller integration architecture (Das, et al., 2013)](image-url)
types of data can be loaded into them. The loading of individual JTAG instructions into scan chains can be blocked based on the credentials of the user. Security strength is dependent on the initial authentication protocol. This security mechanism minimizes the risk of broad distribution of keys by restricting common keys to lower privilege levels. All security privileges can be set dynamically by the developer. The hardware modifications are compliant with IEEE 1149.1 standard and have minimal timing overhead.

(Das, Ege, et al., 2013) described about the security of industrial test compression schemes against differential scan attacks. Test compression is widely used in the semiconductor industry for testing complex circuits in short time without compromising on test quality. It shows that tools using X-masking and X-tolerance are vulnerable and they leak information about the secret key. Attack success rates for scan structure containing a maximum of 32 scan chains and 32 active slices. A noise injector counter measures is proposed and its security properties were analyzed.

(Baranowski, 2013) proposed a solution for multilevel access management in reconfigurable scan networks (RSNs). Accessibility of RSNs are restricted by extending the TAP with a sequence filter. Filter is enabled by a single fuse. Multilevel access management is employed at both internal and external interface of a scan network. It is employed in core-based design flows and allows fine-grained access management. This scheme can be combined with authentication mechanisms to provide logical security without the need to redesign the scan network. This approach does not affect the access time and it is well suited for core-based designs.

(Da Rolt, et al., 2014) discusses about the past and present of the testing and
security. It describes about the scan based attacks on symmetric and public key cryptographic circuits in the presence and absence of DFT techniques. Existing solutions for the scan-based attack are evaluated for determining protection against this type scan attacks. In addition to the scan chain, JTAG is another testing technique that is vulnerable to the side channel attacks. Most of the scan based attacks target on the registers that stores immediate result of the computation and hence they are strong. Test interface has two security drawbacks, they make scan-based attack easier and they can be used to upload corrupted firmware updates in the non-volatile memories or read out internal contents and use this data to duplicate the device. Various countermeasures for both scan-based and JTAG attacks are also discussed here. Test wrappers are built around the CUT to control the access to the test architecture. Figure 3.12 shows the different attack scenarios. It shows that a potential hacker can shift-in corrupted data and shift-out confidential data during the test mode of operation. Figure 3.13 shows the various categories of countermeasures proposed including the secure test wrappers technique and the attacker classes.

(Ma and Wu, 2014) proposed a low cost error detection and recovery (LOEDAR) scheme to protect from side-channels attacks. This scheme retains the efficiency of Montgomery ladder algorithm and shows resistance towards both environmental-induced faults and as well as attacker-introduced faults. Architecture for LOEDAR is shown in Figure 3.14. It composed of an EDR/ECSM module, a coordinate transformation module, an accumulation module, a point verification module and a register file. This scheme is compatible with most of existing countermeasures
against various power analysis attacks.

(Tena, 2014) proposed a technique for improving the differential power delivery
network (DPDN) of differential logic gates used in the cryptographic applications. DPA (Differential Power Analysis) is one of the available side-channel through which attacker can attack the cryptocircuits and get the critical information of the device. To protect security devices against this issue, differential logic styles with (almost) constant power dissipation are widely used. Possible attacks on cryptocircuits using DPA and their countermeasures are discussed here. This approach uses two mechanisms: single-switch and double-switch solution to remove the charge in the pull-down of a differential gate and eliminate memory effect. It improves the DPA-resistance of the gate with minimum performance degradation.

(Ramya and Saravanan, 2015) proposed a technique to secure digital ICs from various scan based attacks. In this scheme an additional inverter is used in scan-chain architecture to flip the scan chain. Flipped scan-chain increases the switching of scan output and increases the complexity of brute-force attack to retrieve secret data. It compares the actual responses with the expected responses within the chip.
area instead of scanning-out and comparing the response within the ATE. This approach results in negligible area overhead with high security level and can be applied for all scan testing. Also this design does not impact on the quality of the test and diagnosis of fault.

(Jahangiri and Press, 2008) have tried to explore test patterns for IC’s that are both secure and have very high coverage. Secure applications often require high test quality with increasing demands at 65 nm and below. A test method that is secure is necessary such that the test can be conducted outside of a costly secure test environment. Logic BIST is the most secure test method. However, for some devices, it does not provide a high enough test quality or support newly desired fault models.

3.5 Summary

This Chapter discussed the various state-of-the-art methods in test pattern compression and secure testing of VLSI designs. Many of the methods which has a feature adopted by the proposed method are shown with the figures. Each method has a trade off associated with it. Chapter 4, gives more analysis on the types of the existing methods and gives a categorized analysis and classification of these methods based on their features and draw backs. This analysis provides way to the scope of the proposed research.