Crypto Keys Based Secure Access Control for JTAG and Logic BIST Architecture

Ramesh Bhakthavatchalu [#1], Nirmala Devi.M [#2]

[#] Electronics and Communication Engineering, Amrita School of Engineering,
Amrita Vishwa Vidyapeetham, Coimbatore, India.
[1] rameshb@am.amrita.edu
[2] m_nirmala@cb.amrita.edu

Abstract— A technique to provide programmable secure access to the scan based Logic Built in Self-Test (BIST) structures is proposed. Joint Test Access Group (JTAG) interface is the major test access method used in VLSI IC's. At the same time, it can be misused as a means to access and hack the hardware circuitry of the IC. It is addressed in this method to prevent unauthorized users from hacking the JTAG interface and interfering in the Logic BIST test functions. A two stage, multiple crypto algorithms based separate authorization schemes are used. A configuration register can be programmed to select the level of security to a specific user group. Different crypto algorithms can be chosen, with user specifiable key lengths. A challenge response protocol is employed to authenticate the user and corresponding accessibility. All the features included are compliant with the IEEE JTAG standard 1149.1. This technique is applied on ISCAS-89 and ISCAS-99 benchmark designs with the help of Cadence Encounter true time 13.1 design automation tools and results are shown. A small amount of (less than 2 to 5%) increase in area reported for implementing the security features.

Keyword- Logic BIST, hardware security, boundary scan, scan chain, DFT, at-speed testing

I. INTRODUCTION

The current state of IC (Integrated Circuit) testing is evolving continuously. Logic Built In Self-Test (BIST) is one of a latest technique where any electronic hardware unit, chip or circuit can be made to test itself by embedding a small extra circuitry in to it. It is a major technique used to test current day electronic designs of deep submicron technologies. Logic BIST [1, 2, 3] is considered as the most suitable testing technique for System on Chip (SoC) designs. As density of devices in a single IC is constantly increasing leading to SoC designs, there is an equally growing demand to ensure the security and reliability of these devices both in the design aspect and the testing aspect. The securities in chips deter the prospective attackers from performing unauthorized procedures.

It is common practice that most of the SoC devices employ third party Intellectual property (IP) designs from multiple vendors and the fabrication is done by third party foundries. Since the design and manufacturing processes are performed by different independent parties there is a possibility of overbuild, copy and or modifications to the design [4]. These breaches by third party are mostly clandestine and are difficult to prove. Also on the field, much of side channel attacks are possible to destroy the normal functioning of an IC or to steal the data passing through the system. For example, side channel attacks on an IC fitted in an Automatic Teller Machine (ATM) can tap the secret numbers and passwords of the users [5]. Security issues arise when the intended operation of a circuit is tampered and have a discrepancy in real time operation [6]. Other than the conventional design attacks, new kind of attacks were developed recently targeting through the test ports and architectures.

In past few decades JTAG/IEEE 1149.1 has evolved as the single standard interface to test and debug a device, board and at system level [7]. Many configuration and debug operations are usually performed through this JTAG interface. In many electronic systems remote access is performed by the TAP of the chips connected through a computer on the internet. For example, the firmware updates in a set top box occur through the JTAG port [8]. Open access characteristics of JTAG features can be exploited by malicious users as a backdoor for launching attacks such as firmware modifications and corrupt the system, duplicate the system design, etc creating serious threat to the electronic device's security [9, 10]. There is a possibility that the data confidentiality and IP protection can be broken during the process of testing [11]. Easy access to debug ports and module's test structures can be used to steal the contents of the IP and modify the firmwares [12]. Thus the test access mechanism are critical components that not only affect production and operation of the system/device, but also affects system security [13].The need for security of the JTAG port has been introduced[14] in last decade and methods to prevent unauthorized access to the device through the JTAG port were suggested. Techniques suggesting for security from the side channel attacks on the scan chains and BIST circuitry are also under research. This paper suggests a dual stage security, one at JTAG level and other at the Logic BIST structure thus providing increased security.

The rest of the paper is organized as follows. Section II of this paper discusses the various security issues of the test structures and more of the previous techniques suggested in the literature. Section III proposes a scheme to access the JTAG and then in to the Logic BIST test structure. Section IV discusses the implementation details and performance of the new scheme. Section V concludes the paper.

II. TEST AND HARDWARE SECURITY

Enabling disabling and controlling the different internal test structures like memory BIST, Logic BIST of many different modules inside a large SoC chip is usually performed through the JTAG interface. An internal self-test circuitry like Logic BIST may isolate the scan chains from side channel attacks but needs a proper access control to secure itself from an external hacker. So the security issues are equally threatening to the test structures as well, embedded inside the IC.

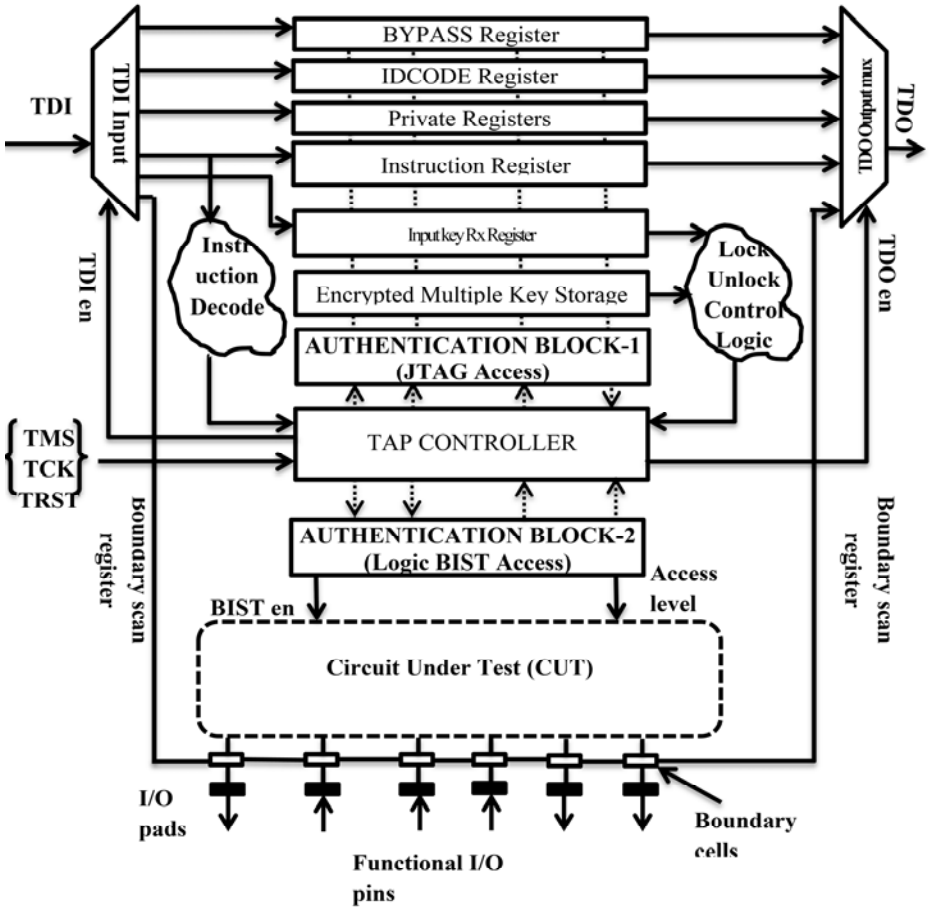

Fig. 1. Typical JTAG structure and dual stage security blocks added

General structure of JTAG architecture is shown in Fig.1. A TAP controller controls the overall operation of the JTAG structure. Group of registers store the standard details of the IC like the Vendor ID, Device ID, Instructions ID, etc. to perform the mandatory operations as per the IEEE standards. An instruction decoder helps in decoding the instructions entered through the Test Data Input (TDI) port and boundary cells added to the corresponding input/output pins are mandatory structures added as per the IEEE 1149.1 standard. The structure also shows the two proposed authentication modules which help in implementing the proposed technique. The details of these modules can be found in next section.

Techniques presented in literature that help in hardware security for both the design and test domain are given below. A method to prevent a hacker from accessing the JTAG registers of an IC is by having a lock and secret key register. Security methods based on secret digital keys is a technique mostly used but has the vulnerability depending on the hardware implementation and key storage [15]. Hardware metering is a method of security protocol to uniquely tag each IC after manufacturing which can help in detecting hardware piracy [16]. Many methods to prevent and identify cloned IC's including physically unclonable functions (PUF) are also in development [17]. While hardware metering is used to tag a physical device, methods such as digital water marking are used to tag a design itself. Multiple devices can have the same water mark but cannot have the same

tag of digital metering technique. Digital water marking is another major security technique embedded into the design which when extracted can be used to detect hardware piracy of VLSI designs and establish legal ownership [18]. A method to watermark digital designs at the HDL level was presented in [19]. Side channel attacks to a chip by directly taping its pins or signals to either gain access to tamper the wires or data theft by simple measurements is another kind of hardware attack [4].

Increase in the powerful features being deploy through the JTAG interface has left the testing platform vulnerable to malicious users [15, 20]. In remote networked system maintenance, an attacker may crack the computer system and get access to the test port [21]. Secure JTAG port has been introduced to limit the device access to only authorized users in order to ensure the security of sensitive information without disturbing the debugging functionality [22]. Schnorr and etal presented a security method by modifying the TAP controller architecture [8]. Mitigating the side channel attacks by masking the internal power consumption from the attacker is discussed in [23]. Error detection and recovery of the hardware attacks using Elliptic Curve Cryptography is discussed in [24]. Security problems during industrial test compression have been analyzed in [25]. Possible attacks on cryptocircuits using differential power analysis (DPA) and their protection measures are discussed in [26].

Most of the above security approaches need design modifications and sometimes have considerable area, power overhead and may cause timing issues. For example, implementing a crypto-algorithm inside a VLSI IC increases the area to a large extent as if a crypto processor is added in to the design. A possible solution is to have the crypto keys stored inside the IC instead of actually implementing a cryptographic hardware inside the IC. In the proposed method key encryption and decryption are performed as part of the access control process but they are not part of the security module implemented inside the IC. Instead the crypto-keys are stored inside a register and the different algorithms for different access levels are made programmable. This reduces the area and power consumption overhead tremendously comparing to previous methods which try to implement the crypto algorithm inside the design.

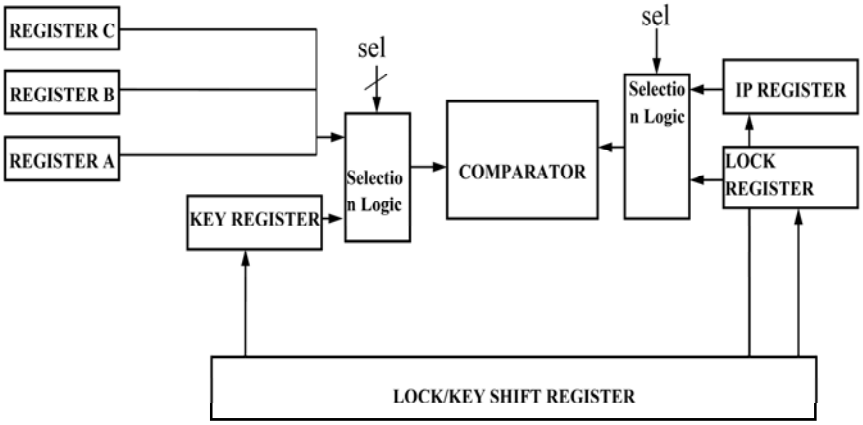

Fig. 2. Block diagram of the password key based access system

This paper describes the specific security features built upon the JTAG and Logic BIST architecture. The crypto keys based security feature increases the difficulty level for a hacker to access the internal details of the IC. The circuits of interest in this paper are the standard ISCAS'89 and ISCAS'99 benchmark designs. Complete boundary scan flow is implemented and Logic BIST circuitry is built on all the benchmark designs and the proposed security feature is added to the output design netlist. The results are tabulated and compared with the literature.

III. PROPOSED DUAL STAGE SECURITY SCHEME

The proposed architecture uses a dual stage and multilevel controlled entry structure to access and run the Logic BIST. Users are classified in to multiple ranks and based on their ranks access and privileges are enabled. To access the Logic BIST structures, one has to go through the boundary scan controlled entry which is the first stage of security. A locking and unlocking mechanism is employed with a password (key) protected entry scheme. Multiple users of different ranks will have different passwords provided in advance. The multiple user ranks can be proposed as below.

A User/test engineer will be able to access the boundary scan registers and run the boundary scan instructions but may not be able to modify/program any of the register contents other than giving inputs and checking the outputs.

A Design Engineer will have better priority that he will be able to modify the values stored in the registers including the IDCODE register.

An architect gets the top priority and will be able to do modifications to hardware operations like re-configuring the size of private register for the boundary scan public or private instructions.

The first stage of security module is added in the JTAG architecture and a second stage of security module is implemented at the Logic BIST structure.

A. JTAG Lock/Unlock Mechanism – Secret Keys Module

A key lock and unlock mechanism is used in conjunction with a secret key password based access. Other than the mandatory instructions specified for a TAP controller by the IEEE standard, the proposed architecture consist of two additional private instructions: LOCK and UNLOCK. When the LOCK instruction is active, then TAP controller maps all the instructions except UNLOCK instruction to a harmless bypass logic until the UNLOCK instruction with a valid key code is applied [21]. In addition to locking TAP controller, it also provides different levels of access to the system. Once the tap controller gets unlocked by entering the correct KEY, the user have to enter a security code which selects the privilege levels of access that user can have on the system functions.

In addition to the mandatory structures shown in Fig.1, the proposed architecture of this dual-stage security system consists of a key/lock shift register, a key register, a lock register, a comparator, private instruction register, and associated multiplexers. It also includes three level selecting registers (register X, register Y, register Z) with keys embedded in it. Level select registers will determine the level of access given to the users. Fig.2 shows the block diagram of the password key based access system. There are four levels of protection are suggested to access the JTAG structure.

Level 1 (Locked level): All instructions are sent through BYPASS register. System remains completely locked, i.e. user does not have any access to the system. Even circuit debugging is not possible.

Level 2 (User level): This level allows only for executing running the boundary scan instructions and circuit debugging. No writing in to the registers possible.

Level 3 (Designer level): This level allows circuit debugging and writing into some of the internal registers.

Level 4 (Architect level): This level does not add any protection to the device. User can access any data in the device and may even change the hardware structure. For example, writing in to the private registers, changing the size of a programmable register.

The aspects of protection are tabulated and shown in Table I. The authenticity property indicated whether an authentication is given to the corresponding user, secrecy property indicates the accessibility to the internal registers and modifying its contents and integrity property indicates the capability to access the hardware and modify the design specific functions of the device.

TABLE I. PROTECTION LEVELS AND SECURITY TYPE

Levels	Authenticity	Secrecy	Integrity
Level 1	No	No	No
Level 2	Yes	No	No
Level 3	Yes	Yes	No
Level 4	Yes	Yes	Yes

B. Programmable Crypto Keys based Security Module

1) Logic BIST access steps: A crypto keys based authentication module is used as the second stage to access the Logic BIST architecture. A configuration register, storage module, a decoder and a comparator are the blocks constituting the authentication module. A security configuration register is a 128 bit register that is used to program the security features.

The first step of the LBIST private instruction is that the user inputs a 128 bit data into the logic BIST security configuration register through the TDI pin. At the same time, the contents of the crypto key security register will be serially shifted out via the TDO pin. The LSB 8 bits or MSB 8 bits of this security register can be made programmable to specify the security features based on bit 8 of the register.

The user will encrypt the 128 bit data using the private key already provided. All the 3 categories (3^{rd} party user, designer and architect) of the users will use their corresponding private key assigned to them and the corresponding crypto algorithm. It is suggested that this 128 bit data may be the original seed of the LFSR's used in the Logic BIST structure [27].

The calculated encrypted value will be then re-entered through the TDI pin and it is compared with the value in the storage module. If this value matches with the value in the storage module, then an authentication pass signal will be issued, otherwise an authentication fail signal will be given out. Authentication pass signal with the user id will allow the user to access specific modules in the internal core.

2) Security Configuration Register: A crypto keys based authentication module is used as the second stage to access the Logic BIST architecture. Fig. 3 shows the configuration register details. Security configuration register is a 128 bit register that is used to ensure the security of the design. The value present in this register determines which cryptographic algorithms have to be used, key length and level of access. Configuration register consist of a mode selection bit, level selection bits, cryptographic algorithm selection bits and key selection bit. Based on these 8 bits of LSB (MSB), corresponding encrypted value will be selected from the storage module. Storage module consists of a number of encrypted keys and selection is made on the basis of 8 bits (MSB OR LSB) values in the configuration register. Similar to the JTAG security module multiple user level access mechanism is maintained in this module also.

The bits 8-0 in the security configuration register are decoded as shown in Fig. 3 are specified below.

Mode selection bit: Out of the 128 bits, 8^{th} bit determines the mode of operation i.e. MSB or LSB mode. If the bit is 0, then 8bit of LSB is used. If the bit is 1, the 8 bit of MSB is used.

Level selection bits: 7^{th} (120^{th}) and 6^{th} (121^{th}) bits are used to select the level of access. There are four levels of access such as locked (level 1), user (level2), designer (level3) and architect (level 4).

Cryptographic algorithm selection bits: 5^{th} (122^{th}), 4^{th} (123^{th}) and 3^{rd} (124^{th}) bits are used to select different cryptographic algorithms.

Key selection bits: 2^{nd} (125^{th}), 1^{st} (126^{th}), and 0^{th} (127^{th}) bits are used to select the key length for text data.

Table II shows the programmable size and key details for the different supported crypto algorithms that can be employed in the method. These can be modified as per the requirements of the different implementations.

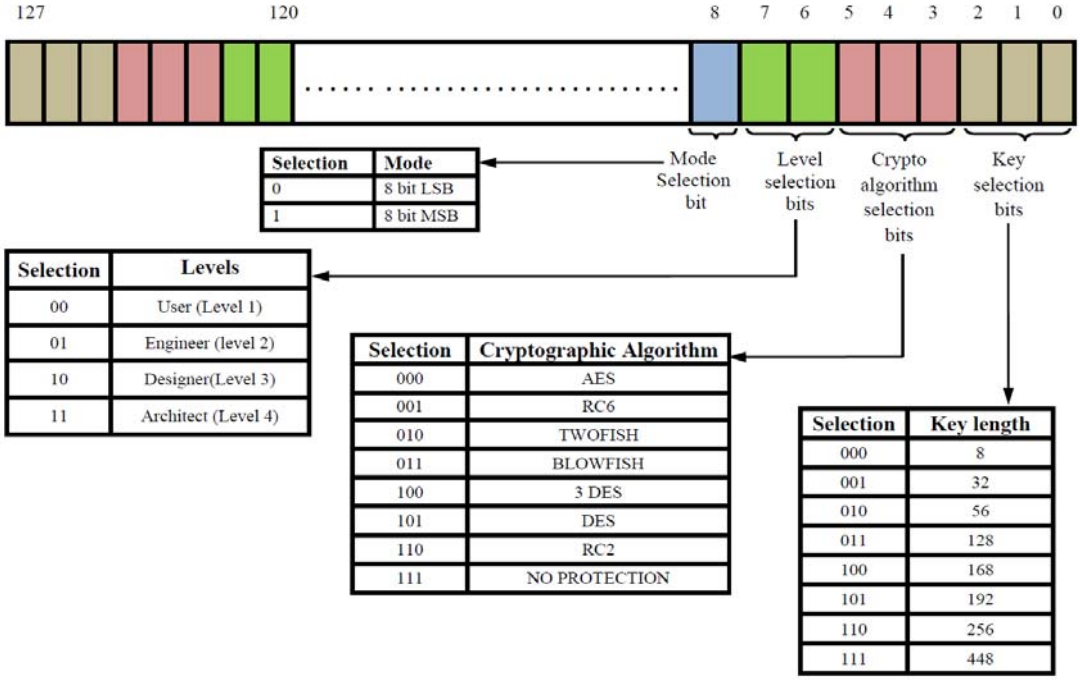

Fig. 3. Security Configuration Register Details

Any algorithm and its key size and data size can be added or discarded or modified.

TABLE II. List of Supported Crypto Algorithm Details

Type of Algorithm	Text data	Level	Key length
AES	128	All	128,198, 256
RC6	128	All	128,198, 256
Two Fish	128	All	128,198, 256
Blow Fish	64	Level 2 & 3	32, 128,448
3DES	64	Level 1 & 2	168
DES	64	Level 1 & 2	56
RC2	64	Level 1 & 2	8, 128

IV. RESULT & ANALYSIS

All the designs and security modules were written in Verilog HDL. All experiments were conducted on ISCAS'89 and ISCAS'99 benchmark designs on a computer with 3.1 GHz CPU and 8GB memory. All the simulations are performed in Modelsim RTL simulator. These designs were synthesized using 90nm standard cells library in Cadence Encounter Tool. The boundary scan vectors simulation is performed in Cadence Encounter Test Architect.

A. JTAG security module Insertion Results Analysis:

Table III shows the boundary scan and design details on the ISCAS'89 benchmark sequential circuit designs. The first column shows the name of the design. The second and third columns show the number of input and output ports of the designs respectively. Fourth column shows the number of total no of nets in the design. Fifth and sixth columns show the number of boundary cells added as part of the JTAG flow. Area of the design, power estimation, no of gates synthesized and no of Flip-flops present in the processed designs were also shown in the next 4 columns. The last two columns show the number of boundary scan test vectors simulated for the IEEE 1149.1 standard instructions (including the PRIVATE instruction) and for the EXTEST instruction. All the '89 benchmarks have single clock domain and single reset port for which the boundary cells are inserted. Table V shows the same above details for ISCAS'99 benchmark designs.

TABLE III. JTAG Flow details on ISCAS'89 benchmarks

Design	# PI	# PO	Nets	# BCells		Clk & Rst	Area (nm^2)	Power (mw)	No of gates	FFs	Boundary scan vectors	
				Bc_ in	Bc_ out						1149	EXTEST
s27	11	2	3966	4	1	1	110391	2.503	1705	67	3354	75
s298	10	7	5214	3	6	1	149009	5.105	1780	87	3415	264
s344	16	12	6207	9	11	1	254763	8.594	1825	104	3574	560
s349	16	12	6207	9	11	1	254763	8.594	1825	104	3574	560
s382	10	7	5626	3	6	1	149082	5.109	1799	94	3415	264
s386	14	8	5258	7	7	1	197020	4.847	1798	85	3486	360
s420	25	2	5865	18	1	1	245131	4.895	1803	94	3550	439
s444	10	7	5629	3	6	1	149083	5.108	1802	94	3415	264
s510	26	8	6322	19	7	1	312397	7.214	1878	96	3654	720
s526	10	7	5706	3	6	1	149104	5.108	1810	94	3415	264
s641	42	25	9641	35	24	1	629687	1.928	1990	160	4133	2328
s713	42	24	9527	35	23	1	620067	1.792	1984	158	4118	2288
s820	25	20	7612	18	19	1	418216	1.060	1954	119	3820	1159
s832	25	20	7586	18	19	1	418211	1.060	1951	119	3820	1159
s838	41	2	8076	34	1	1	399124	7.682	1920	126	3774	1335
s953	23	24	9462	16	23	1	437734	1.663	2056	149	3852	1243
s1196	21	15	8281	14	14	1	331976	1.066	2057	118	3689	815
s1238	21	15	8297	14	14	1	331982	1.013	2061	118	3689	815
s1423	24	5	10368	17	5	1	274721	6.628	2093	159	3596	560
s1488	15	20	8086	8	19	1	322876	1.102	2091	110	3680	859
s5378	42	50	22779	35	49	1	872042	4.336	2732	367	4508	3328
s9234	43	40	19612	36	39	1	785041	2.676	2498	317	4372	3003
s13207	70	153	58412	62	152	1	2135304	8.985	3993	1018	6445	10304
s15850	84	151	57939	77	150	1	2250747	9.416	4393	948	6611	12240
s38417	35	107	118955	28	106	1	1368786	6.533	7250	1862	5265	5139
s35932	42	321	144610	35	320	1	3495307	2.096	8541	2461	8573	14168
s38584	45	306	130854	38	304	1	3367482	1.679	9091	1978	8375	13759

TABLE IV. Security Overhead Performance on ISCAS'89 benchmarks

Design	Without security		With security		Increased %	
	Area(nm^2)	Power(nw)	Area(nm^2)	Power (nw)	Area(nm^2)	Power(nw)
s27	106318	2331200.965	110391	2503894.615	2.339918603	4.385865905
s298	144936	4933199.168	149009	5105892.818	1.723043315	2.103777536
s344	250690	8421901.834	254763	8594595.484	1.000638284	1.239233384
s349	250690	8421901.834	254763	8594595.484	1.000638284	1.239233384
s382	145009	4936538.032	149082	5109231.682	1.722185073	2.102373821
s386	192947	4674698.830	197020	4847392.48	1.297713064	2.218456051
s420	241058	4722985.604	245131	4895679.254	1.040365694	2.19609458
s444	145010	4935889.942	149083	5108583.592	1.722173323	2.102646142
s510	308324	7041457.062	312397	7214150.712	0.814527242	1.479872843
s526	145031	4936159.078	149104	5108852.728	1.721926593	2.102533045
s641	625614	19108759.254	629687	19281452.9	0.402447211	0.548612913
s713	615994	17754514.236	620067	17927207.89	0.408716478	0.590300496
s820	414143	10433161.236	418216	10605854.89	0.607180316	1.001874797
s832	414138	10432287.778	418211	10604981.43	0.60718762	1.001958141
s838	395051	7510102.973	399124	7682796.623	0.636409481	1.388348221
s953	433661	16461386.267	437734	16634079.92	0.579949909	0.636482345
s1196	327903	10495090.345	331976	10667783.99	0.76612071	0.99600074
s1238	327909	9960378.172	331982	10133071.82	0.766106757	1.049110104
s1423	270648	6456205.800	274721	6628899.45	0.927269588	1.612634615
s1488	318803	10855901.498	322876	11028595.15	0.787883328	0.963101784
s5378	867969	43196409.873	872042	43369103.52	0.290275762	0.24316666
s9234	780968	26593784.265	785041	26766477.91	0.322548903	0.394592467
s13207	2131231	89686268.603	2135304	89858962.25	0.118343195	0.117213343
s15850	2246674	93989945.712	2250747	94162639.36	0.112266443	0.111850148
s38417	1364713	65164059.783	1368786	65336753.43	0.184737627	0.161276838
s35932	3491234	209467521.251	3495307	209640214.9	0.072263293	0.05020802
s38584	3363409	167737710.851	3367482	167910404.5	0.075008366	0.062693755

TABLE V. JTAG Flow details on ISCAS'99 benchmarks

Design	# PI	# PO	Nets	# BCells		Clk & Rst	Area (nm^2)	Power (nw)	No of gates	FFs	Boundary scan vectors	
				Bc_ in	Bc_ out						1149	EXTEST
b01	10	3	4281	2	2	2	110458	2894188.306	1735	70	3355	104
b02	9	2	3965	1	1	2	91198	2174524.642	1712	66	3326	55
b03	12	2	5511	4	1	2	120259	2683895.559	1773	89	3368	88
b04	12	2	6000	4	1	2	120351	2616623.967	1817	93	3368	88
b05	9	7	7782	1	6	2	139891	3550868.848	1992	106	3401	255
b06	10	5	4479	2	4	2	129681	4265777.906	1736	75	3385	184
b07	9	2	5998	2	1	2	91602	2172135.399	1852	89	3326	55
b08	10	2	4786	2	1	2	100936	2278742.654	1744	78	3340	64
b09	10	2	5627	2	1	2	101094	2282207.551	1788	91	3340	64
b10	16	4	5711	8	3	2	177904	4445260.252	1833	87	3454	240
b11	10	2	6800	2	1	2	101393	2288853.454	2004	88	3340	64
b12	10	4	13291	2	3	2	121703	3925033.698	2310	183	3370	144
b13	11	8	7489	3	7	2	168603	5617893.283	1889	119	3444	315
b14	9	5	26065	1	4	2	124928	4412271.296	3752	233	3371	175
b14_1	9	5	26157	1	4	2	124935	4084263.564	3771	233	3371	175
b15	13	7	40050	5	6	2	185084	5820206.195	4740	362	3457	303
b_15_1	13	7	39978	5	6	2	185089	5761454.787	4723	362	3457	303
b17	13	7	40050	5	6	2	185084	5818084.471	4740	362	3457	303
b17_1	13	7	39978	5	6	2	185089	5746750.975	4723	362	3457	303
b18	9	5	26065	1	4	2	124928	4563547.66	3752	233	3371	175
b18_1	9	5	26157	1	4	2	124935	4083951.812	3771	233	3371	175
b19	9	5	26065	1	4	2	124928	4563547.66	3752	233	3371	175
b19_1	9	5	26157	1	4	2	124935	4562223.652	3771	233	3371	175
b20	9	5	26065	1	4	2	124928	4563547.66	3752	233	3371	175
b20_1	9	5	26157	1	4	2	124935	4084263.564	3771	233	3371	175
b21	9	5	26065	1	4	2	124928	4563547.66	3752	233	3371	175
b21_1	9	5	26157	1	4	2	124935	4567969.106	3771	233	3371	175

TABLE VI. Security Overhead Performance on ISCAS'99 benchmarks

Design	Without security		With security		Increased %	
	Area(nm^2)	Power(nw)	Area(nm^2)	Power (nw)	Area(nm^2)	Power(nw)
b01	106385	2721494.656	110458	2894188.306	2.3384661	3.772102892
b02	87125	2001830.992	91198	2174524.642	2.846381126	5.083955932
b03	116186	2511201.909	120259	2683895.559	2.143797511	4.079718467
b04	116278	2443930.317	120351	2616623.967	2.142123622	4.188998911
b05	135818	3378175.198	139891	3550868.848	1.837413644	3.053209373
b06	125608	4093084.256	129681	4265777.906	1.984947742	2.528578214
b07	87068	1999441.749	91602	2172135.399	2.833471789	5.089832664
b08	96863	2106049.004	100936	2278742.654	2.564727879	4.840187721
b09	97021	2109513.901	101094	2282207.551	2.560616821	4.832484129
b10	173831	4272566.602	177904	4445260.252	1.43916068	2.424009273
b11	97320	2116159.804	101393	2288853.454	2.552872994	4.817776543
b12	117630	3752340.048	121703	3925033.698	2.117822771	2.754137547
b13	164530	5445199.633	168603	5617893.283	1.519758669	1.908385613
b14	120855	4239577.646	124928	4412271.296	2.062024117	2.442575392
b14_1	120862	3911569.914	124935	4084263.564	2.061906201	2.643925353
b15	181011	5647512.545	185084	5820206.195	1.382559159	1.840828157
b_15_1	181016	5588761.137	185089	5761454.787	1.382521294	1.859948815
b17	181011	5645390.821	185084	5818084.471	1.382559159	1.841511828
b17_1	181016	5574057.325	185089	5746750.975	1.382521294	1.864796481
b18	120855	4390854.010	124928	4563547.66	2.062024117	2.35969621
b18_1	120862	3911258.162	124935	4083951.812	2.061906201	2.644132516
b19	120855	4390854.010	124928	4563547.66	2.062024117	2.35969621
b19_1	120862	4389530.002	124935	4562223.652	2.061906201	2.360397185
b20	120855	4390854.010	124928	4563547.66	2.062024117	2.35969621
b20_1	120862	3911569.914	124935	4084263.564	2.061906201	2.643925353
b21	120855	4390854.010	124928	4563547.66	2.062024117	2.35969621
b21_1	120862	4395275.456	124935	4567969.106	2.061906201	2.357358362

Two line graphs Fig.4 and Fig.5 are shown to depict the power and area overhead reduction with respect to the size of the designs. X-axis indicates the name of the different designs as per their list numbers. Y-axis shows the overhead in percentage.

B. Logic BIST security module Insertions Analysis.

The comparative results after inserting the dual stage security modules in the existing flow is shown in Table IV for ISCAS'89 designs and in Table VI for the ISCAS'99 designs.

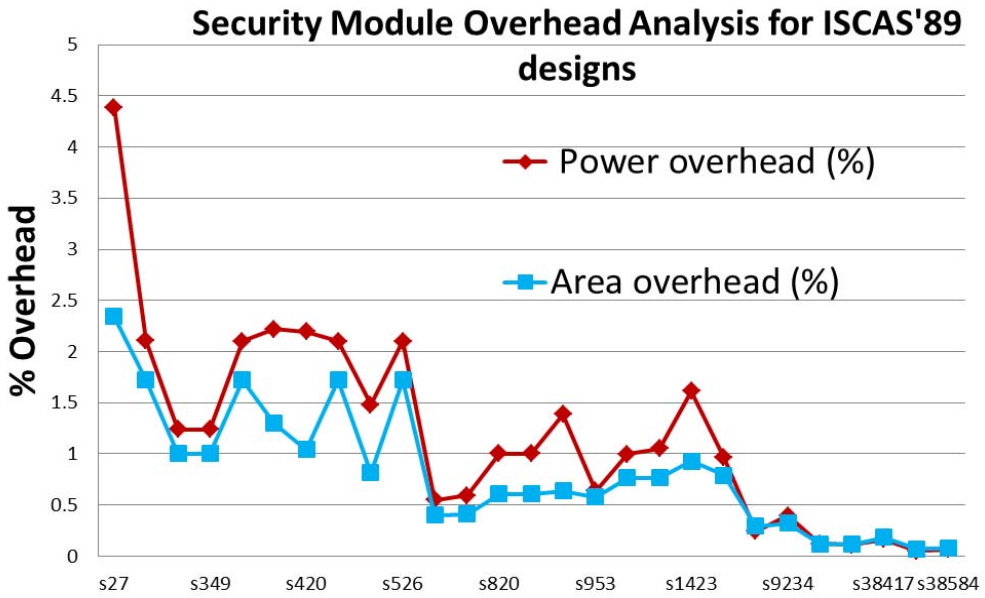

Fig. 4. Area and Power overhead on ISCAS'89 design

For better analysis in the line graphs are shown in Fig. 4 and 5. It is shown that the power and area overhead is very small (ISCAS'99 – power overhead < 5% and area overhead < 2.75 %) (ISCAS'89 – power overhead < 4.5% and area overhead < 2.5%) even for these small sized bench mark designs. As the design size increases the percentage of overhead reduces. It can be clearly seen that for current day VLSI designs this projection will lead to very minimal or negligible overhead.

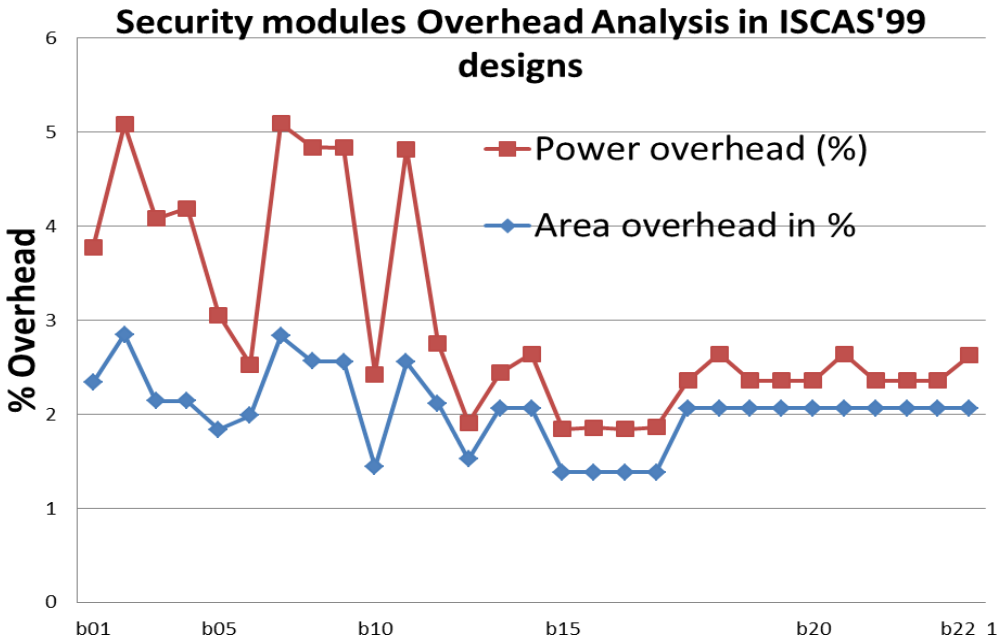

Fig. 5. Area and Power overhead on ISCAS'99 designs

Table VII shows the performance metrics of this method in comparison to the previous methods. The decode difficulty, number of bits and levels to crack are increased while the area and power overhead are reduced. Programmable crypto keys are implemented in the current method whereas an entire crypto processor is proposed in the previous methods leading to a large area and power overhead.

TABLE VII. Security Performance Metrics

Difficulty Level	Ref.[15]	Ref. [22]	Proposed Method
No of bits to crack	32	32	1024
No of levels	4	4	16
Crypto	Yes	Yes	Yes
Design overhead	High	High	Low
Decode Difficulty	Fixed	Fixed	Programmable

V. CONCLUSION

The In this paper a mechanism to enforce a dual stage multi-level privilege security system was proposed for the JTAG boundary scan standard and Logic BIST structure. This method has the flexibility to allow for in the field updates, and debugging of the firmware while maintaining protection to the test and design structures. All security privileges can be set dynamically by the developer. JTAG and Logic BIST test structures are provided with separate access control/authentication modules. Different crypto algorithms with user specifiable key lengths are also suggested. Major highlights of this work are,

- Complete implementation details on ISCAS-89 and ISCAS-99 benchmark designs and results are analysed.
- Comparing many other suggested methods, a small amount of (less than 2 to 5%) increase in area and power reported for implementing the security features. This will be a negligible overhead when adopted on large SoC designs.
- Shown increased cracking difficulty level metrics than similar suggested techniques.

REFERENCES

[1] Michael L Bushnell and Vishwani D Agrawal, “Essentials of Electronic Testing For Digital, Memory And Mixed Signal VLSI Circuits,” Kluwer Academic Publishers, 2002.

[2] L. T. Wang, C. W. Wu and X. Wen, Eds., “VLSI Test Principles and Architectures: Design for Testability,” Morgan Kaufmann, San Francisco, 2006.

[3] L.-T. Wang, C. E. Stroud and N. A. Touba, Eds., “System-on-Chip Test Architectures: Nanometer Design for Testability,” Morgan Kaufmann, San Francisco, 2007.

[4] Mohammad Tehranipoor and Cliff Wang, “Introduction to Hardware security and Trust,” Springer, New York, 2012.

[5] A. Theodore Markettos, “Active electromagnetic attacks on secure hardware,” Technical Report Number 811. University of Cambridge, Computer Laboratory, 2011.

[6] Rosenfeld K and Karri R, “Attacks and defenses for JTAG,” IEEE Design and Test of computers, 2010.

[7] “IEEE standard Test Access Port and Boundary scan Architecture,” IEEE std 1149.1-2001, Institute of electrical and Electronics Engineers, ISBN: 0738129445, 14-jun, 2001.

[8] A. Das, J. Da Rolt, S. Ghosh, S. Seys, S. Dupuis, G. Di Natale, M-L. Flottes, B. Rouzeyre, and I. Verbauwhede, “Secure JTAG Implementation using Schnorr Protocol,” Journal of Electronic Testing: Theory & Applications (JETTA), Springer Science and Business Media, New York 2013.

[9] Keunyoung Park, Sang Guun Yoo, Taejun Kim, Juho Kim, “JTAG Security System Based on Credentials,” Journal of Electronic Testing, vol. 26, issue 5, pp 549-557, October 2010.

[10] David Hely, Kurt Rosenfeld and Ramesh Karri, “Security challenges During VLSI test,” New Circuits and System Conference, 2011.

[11] Jean Da Rolt, Amitab Das, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre and Ingrid Verbauwhede, “Test Versus Security: Past and Present,” IEEE Transactions on Emerging Topics in Computing, Feb 2014.

[12] Kurt Rosenfeld and Ramesh Karri, “Security-Aware SoC Test Access Mechanism,” IEEE 29th VLSI Test Symposium (VTS), 2011.

[13] Sang-Gunn Yoo, Keun-Young Park, Juho Kim, “Software Architecture of JTAG Security System,” WSEAS Transactions on Systems, E-ISSN: 2224-26'78. Issue 8. Volume 11, August 2011.

[14] N G Jacobson, “Intest security circuits for boundary scan architecture,” United States Patent 6, 499,124, Dec-24 2002.

[15] Luke pierce and Spyros Tragoudas, “Multilevel Secure JTAG Architecture,” IEEE 17th International On-Line Symposium, 2011.

[16] Koushanfar F and Gang Qu., “Hardware metering,” Design Automation Conference (DAC), pp 490–493, 2001.

[17] Gassend B, Clarke D, van Dijk M, Devadas S, “Controlled physical random functions,” Proceedings of the 18th Annual Computer Security Applications Conference, pp 148–160, 2002.

[18] Andrew B. Kahng, John Lach, et al., “Constraint-Based Watermarking Techniques for Design IP Protection,” IEEE transactions on computer-aided design of integrated circuits and systems, vol. 20, no. 10, pp.1236 -1252, Oct 2001.

[19] Castillo, E. , Meyer-Baese, U., Garcia, A., Parrilla, L., Lloris, A., “IPP@HDL: Efficient Intellectual Property Protection Scheme for IP Cores,” IEEE transactions on very large scale integration (VLSI) systems, vol. 15, no. 5, pp.578 -591, May 2007.

[20] Luke pierce and Spyros Tragoudas, “Enhanced Secure Architecture for Joint Action Test Group Systems,” IEEE Transactions on Very Large Scale Integration Systems, Volume 21, July 2013.

[21] Novak F, Biasizzo A, “Security Extension for IEEE std 1149.1,” Journal of Electronic Testing: Theory and Applications, 2006.

[22] Pooja Ajay Kumar, P Satish Kumar, Aditi Patwa, “JTAG Architecture with Multi Level Security,” IOSR Journal of Computer Engineering, ISSN: 2278-0661, Volume1, Issue1, May-June 2012.

[23] Orhun Aras Uzun, Selçuk Köse, “Converter-Gating: A Power Efficient and Secure On-Chip Power Delivery System,” IEEE journal on emerging and selected topics in circuits and systems, vol. 4, no. 2, June 2014.

[24] Kun Ma and Kaijie Wu., “Error Detection and Recovery for ECC: A New Approach against Side-Channel Attacks,” IEEE transactions on computer-aided design of integrated circuits and systems, vol. 33, no. 4, April 2014.

[25] Amitabh Das, Barıs Ege, Santosh Ghosh, Lejla Batina and Ingrid Verbauwhede, “Security Analysis of Industrial Test Compression Schemes,” IEEE transactions on computer-aided design of integrated circuits and systems, vol. 32, no. 12, December 2013.

[26] Erica Tena-Sánchez, Javier Castro, and Antonio J. Acosta, "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits," IEEE Journal on emerging and selected topics in Circuits and Systems, vol. 4, no. 2, June 2014.
[27] Ramesh Bhakthavatchalu, Sreeja Krishnan, Vineeth V, Nirmala Devi M, "Deterministic Seed Selection and Pattern Reduction in Logic BIST", Proceedings in 2014, 18th IEEE International VLSI Design and Test Symposium (VDAT), 2014.

AUTHOR PROFILE

Ramesh Bhakthavatchalu received his B.E from Vellore Institute of Technology. He completed his M.E in Applied Electronics from College of Engineering, Guindy, Anna University. Then he served as Senior Design Application Engineer in Cirrus Logic Inc., USA and Syntest Technologies, USA for 8 years. He has taped out 4 designs during his tenure in VLSI Industry. Currently he is working as Assistant professor in ECE department of Amrita Vishwa Vidyapeetham, Amritapuri, India for the past 11 years. His areas of expertise are Design For Testability, FPGA based system design, ASIC design. He has published more than 15 international conference and journal papers in VLSI design and testing area in last 3 years.

Dr. M. Nirmala Devi obtained her B.E. degree in Electronics and Communication Engineering (ECE) in 1990 and M. E. (Applied Electronics) Degree in 1996 from Government College of Technology, Coimbatore, Bharathiar University. She is currently working as the Professor in Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore. She has received her Ph.D degree in the area of VLSI Design of Artificial Neural Networks from Anna University, Chennai. She is the recipient of "Appreciation Award" from Amrita Institute of Technology during the year 2003. Moreover, Marquis Who's Who in the World 2011 distinguishes her as one of the leading achievers from around the country. Furthermore, International Biographical Centre, Cambridge, England has chosen her for inclusion in the prestigious publication "2000 Outstanding Intellectuals of the 21st Century – 2011". Her areas of interest include VLSI Design and Testing, Computational Intelligence, Hardware Security and Trust, Evolvable Hardware and RF System Design. She has published around 55 papers in the International Journals and Conferences in her field of expertise. She has served as the reviewer for a few international conferences and the international journals.