JTAG Architecture with Multi Level Security

Pooja Ajay Kumar[1], P. Sathish Kumar[2], Aditi Patwa[3]
(Department of Electronics and Communication, Amrita School of Engineering, Bangalore)

ABSTRACT : *For in–circuit testing and debugging JTAG (Joint Test Access Group) is one of the most powerful standard architecture of DFT (Design For Testability). But JTAG can also act as a tool for hacking and hence makes the devices vulnerable for attacks. This paper presents a Security mechanism for JTAG and hence prevents the unauthorized users from accessing the private and confidential information of a device. This method is highly compatible with the IEEE 1149.1 standard and requires no modification in the Intellectual Property of an IC. In this paper the standard JTAG Architecture with enhanced security mechanism is described using VHDL.*

Keywords – *JTAG, DFT, Boundary Scan, Security, AES, Authorization, Privilege Levels.*

I. INTRODUCTION

Due to the rapid advancement in microelectronic industry, the role of Integrated Circuits is becoming more and more significant. Testing has become a major challenge in the world of IC's and traditional methods became outdated. In recent years, DFT has become the major tool for testing and hence made the test generation and test application cost effective. JTAG [1] or BST (Boundary Scan Test) is one of the DFT technologies which add boundary scan cells between the I/O pins and the core logic. It provides testing at all levels of hierarchies such as chip, board and system level. JTAG port act as the interaction point between the external world and the processor and it provides access to the internal components; therefore it has to be protected.

JTAG interface provides two types of interactions in which one provides circuit debugging and the other provides access to the internal components which includes even overwriting of internal registers and flash memory. The second type of interaction makes the system prone to unauthorized usage and hacking [2]. To deny the unauthorized users in accessing the features of JTAG port, certain security mechanism has to be provided. The secure JTAG port has been introduced to limit the access to the device in order to ensure the security of sensitive data, without disturbing the debugging functionality.

The paper presents VHDL implementation of a JTAG Architecture with multi level security [3]. This security mechanism provides various privilege levels to the user group which determines exactly what all areas they can access based on their authorization. This Architecture uses AES Encryption/Decryption [5] for private key generation and it uses the Challenge- Response protocol [4, 6] for authorization. The architecture is fully compatible with the IEEE 1149.1 standard and requires no modification in the JTAG Tap Controller.

II. STANDARD JTAG ARCHITECTURE

The standard JTAG Architecture is shown in Fig 1 which consists of hardware elements like Test Access Port (TAP), TAP Controller, Instruction Register (IR), Boundary Scan Register (BSR), Bypass Register (BR) and Idcode Register.

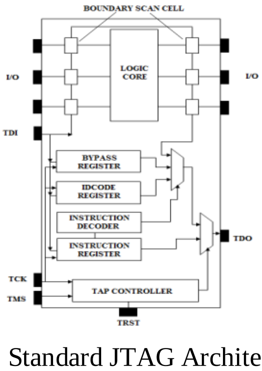

Fig 1. Standard JTAG Architecture

The TAP includes five dedicated pins namely TDI which act as the Test data input, TDO which is the Test data output, TCK which is the Test clock that helps in transferring data and instructions among various registers, TMS which is the Test mode select pin that act as the sole test control input to the Tap controller and TRST for resetting the Tap Controller. The Tap Controller is a 16-state FSM which recognizes the communication protocol and generates the internal control signals used by the Boundary Scan logic. The Tap Controller is shown in Fig 2 and is driven by TCK and TMS only.

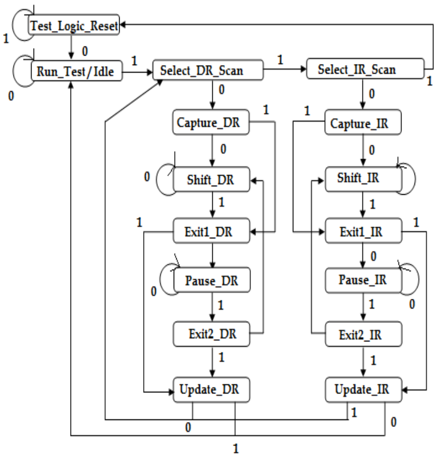

Fig 2. Tap Controller

The Instruction Register allows an instruction to be shifted into the design. The instructions are used to select the test to be performed or the Test Data Register to be accessed or both. The Instruction Register is a shift-register-based design. The three mandatory instructions comes under JTAG are EXTEST, SAMPLE/PRELOAD and BYPASS. Boundary Scan Register consists of all the BS cells on the periphery of the chip. Bypass Register consists of a single shift register stage to shorten the board-level serial scan chain by bypassing some devices while accessing the others. It permits a shortcut between TDI and TDO thereby reduces the software overhead. Idcode Register is an optional register which is basically a 32-bit PISO. It is intended to contain the manufacturer's number and the version number. This helps in verifying that the correct IC is mounted in a correct position or not.

III. PRIVILEGE LEVELS

In the present era of nanotechnology, there exist thousands of devices that provide various services. It can range from an electronic toy to complex processors. JTAG security must be provided to those equipments with confidential data and it will also be inappropriate to add security to the irrelevant ones. The security requirement depends on the application of the device and different points in the product life cycle require different privilege levels. A device will have different phases during its life cycle including development, testing, assembling, shipping etc and during each stage the need for protection increases. In some cases user needs to lower the protection temporarily for some maintenance function. But this feature will be available only to the trusted users. This architecture provides multi privilege levels. The various privilege levels offered by the model are: P1, P2, P3 and P4.

3.1 Unprotected Level (P1)

The developers might need unrestricted access to the device during its development stage. Besides debugging, the device configured to this level also provides access to flash memory and other internal resisters. In addition this level does not offer any protection to the device and the user can access even the secure area of the device.

3.2 Low Protection Level (P2)

The device configured to this level allows circuitry debugging functions, as well as writing into the flash memory and modifying the ROM and internal registers. For the authorized users, the protection level can be lowered to unprotected level if needed.

3.3 Medium Protection Level (P3)

In this level, the only functionality available is debugging. This level limits user access through the JTAG port to certain functions such as testing of chip circuitry and board level interconnections. If requested by a trusted user, the protection level can be lowered temporarily to P2 or P1.

3.4 Maximum Protection Level (P4)

This level stands for the locked state, i.e., no one will be able to access the entire device using JTAG ports. Even the debugging function is not possible in this level. The downgrading of access level is also not possible in P1. This mode is meant for those products which have to be delivered to the customers that contain confidential information.

IV. SECURE JTAG ARCHITECTURE

The architecture presented in this paper gives different privilege levels to different users according to their authorization. Privilege levels and its security will be decided by the designer of the IC. Fig 3 shows the Secure JTAG Architecture. This architecture consists of an Authentication & Authorization Module and an Access Provider. The AAM helps in unlocking the communication protocol and setting the user level. The Access Provider contains a memory element that holds various access levels and it also prevents the entry of harmful data into the device.

During power-up, the entire system will be locked in such a way that the users can’t access any other component other than the AAM Register. Now the user is supposed to complete the Authentication Protocol to unlock the JTAG interface. The Authentication Protocol is a Challenge- Response Identification Protocol and here AES is used for Encryption/Decryption.

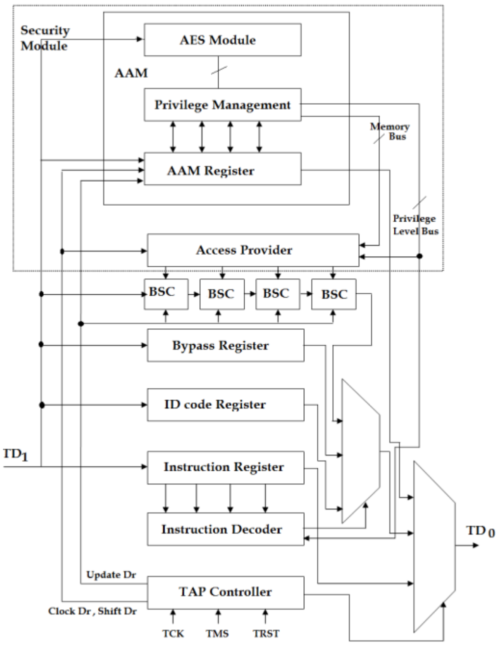

Fig 3. Secure JTAG Architecture

Fig 4 shows the AES Encryption/Decryption process. The bit sequence for representing the request for accessing certain level will be given as the data and the private key will be provided to each user group. The secure JTAG module is capable of generating challenges and verifying responses.

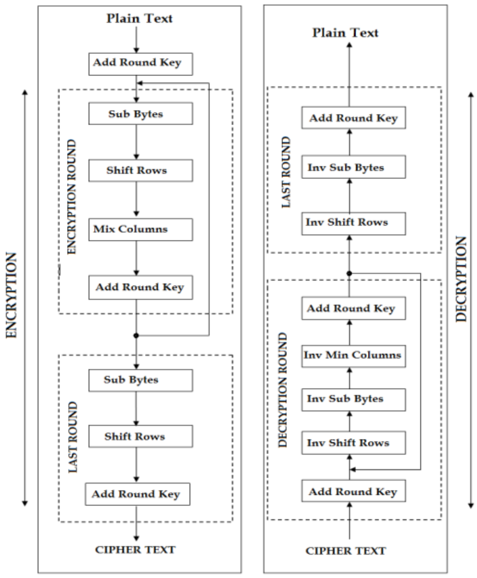

Fig 4. AES Encryption/Decryption

The Access provider's role is user authorization verification upon reception of a challenge and generation of response to the given challenge. AAM will generate the particular privilege level according to the user group, and this will be compared with those access levels stored in the Access Provider. If both match, access will be provided until power-down or else access will be denied.

V. SIMULATION RESULTS

The blocks were modeled using VHDL and simulated using MODEL SIM 10.0d.

5.1 Tap Controller

Fig 5 shows the Simulation Result of Tap Controller. The inputs are TCK, TMS and TRST and the output of this module is the corresponding binary value of the states. State transitions will be based on the value of TMS and takes place at the rising edge of TCK.

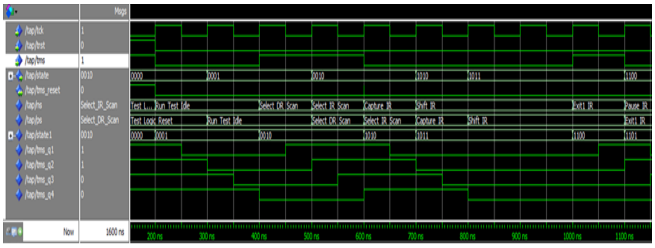

Fig 5. Tap Controller

5.2 EXTEST Selection

Among the three mandatory instructions, EXTEST allows circuitry external to the component package; typically the board interconnects, to be tested. Fig 6 shows the Simulation result of EXTEST selection. The corresponding binary representation for EXTEST instruction is "0000". The value is shifted into the instruction register through TDI during SHIFT_IR state, and during the UPDATE_IR state the output register will be updated with the instruction and EXTEST will be conducted. During this instruction the Boundary-Scan register will be connected between TDI and TDO in the SHIFT-DR state.

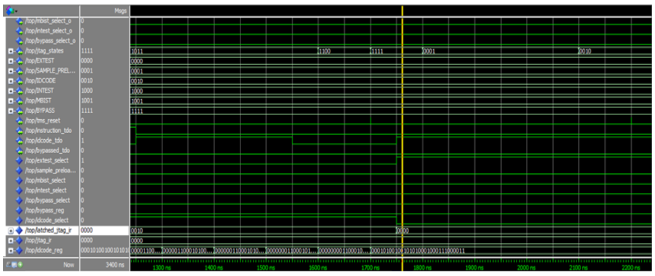

Fig 6. EXTEST Selection

5.3 TDO Multiplexing

Fig 7 shows the TDO Multiplexing. The outputs are TDO, TDO_PAD and TDO_PADE. TDO_PADE shows if TDO driver is activated or not and TDO_PAD gives the corresponding shifted out test vector.

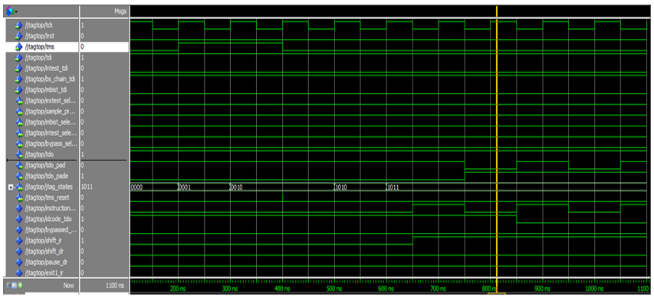

Fig 7. TDO Multiplexing

5.4 AES Encryption/Decryption

Fig 8 Shows the AES Encryption and Decryption. The data Input is 128 bits and here it's given as AABBAABB… and the key is also 128 bits which is 00112233… Section A shows the Data and Key inputs and Section B shows the Encrypted output. Immediately after the Encryption, the cipher text obtained will act as the data input for Decryption. Section C shows the completion of Decryption and the same input AABBAABB… is obtained as the decrypted output.

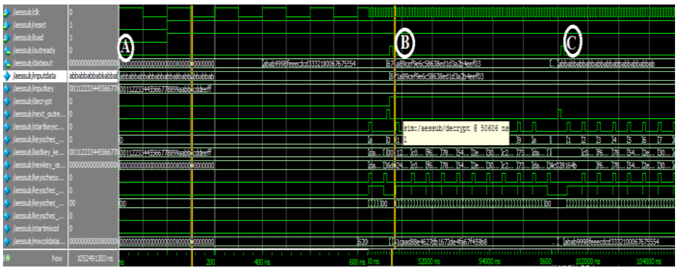

Fig 8. AES Encryption/Decryption

VI. CONCLUSION

This paper presents the VHDL modelling of an IEEE 1149.1 compatible Multi level security mechanism for JTAG. The multi-level security system allows the debugging of the device while maintaining a high degree of protection for the most sensitive part of the IC.

REFERENCES

Standards

[1] IEEE Standard Test Access Port and Boundary Scan Architecture. IEEE Standard 1149.1, 2001.

Journal Paper

[2] Kurt Rosenfeld and Ramesh Karri, Attacks and Defenses for JTAG, *Design and Test of Computers, IEEE*. 2009.

Conference Papers

[3] Luke Pierce and Spyros Tragoudas, Multi-Level Secure JTAG Architecture, *IEEE 17th International On-Line Testing Symposium*, Pages 208-209, 2011

[4] R.F. Buskey and B.B. Frosik. Protected jtag. *In International Conference on Parallel Processing Workshops*, 2006, pages 8 pp.–414, 2006.

Proceeding Papers

[5] Chih-Chung Lu and Shau-Yin Tseng, “Integrated Design of AES Encrypter and Decrypter”, *Proc. IEEE Int. Conf. on Application-Specific Sytems, Architectures, and Processors, (ASAP'02*), pp. 277-285, 2002.

Chapters in Books

[6] *J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, (CRC Press LLC., 1997).*