Secure Scan Chain using Test Port for Tester Authentication

A.Ashna¹, T.Renita Pearlin²

¹ Assistant Professor, Sri Shakthi Institute of Engineering and Technology, L&T By-pass, Chinniyampalayam, Coimbatore – 641062, India
² Assistant Professor, Sri Shakthi Institute of Engineering and Technology, L&T By-pass, Chinniyampalayam, Coimbatore – 641062, India

Abstract— The principal goal of the paper is to reduce hacking from hackers. In order to reduce this access to the scan architecture of known vector is limited by test authentication and also limits the attempts for the application of test vector to observe the result of scan architecture. If the password is correct it move on to the next step otherwise, it again move to login window.

INTRODUCTION

Scan structure also can be applied as underhand means of access for hackers to interrupt chip protection. Test structure used to hack the hardware implementations such us Advanced Encryption Standard, Rivest Shamir Adelman encryption etc. The steady test structure to guard Circuit under test in opposition to experiment-primarily based totally assaults at the same time as keeping a excessive controllability and observability.

There are normally used strategies to offer safety for experiment structure in opposition to capacity assaults. First, the get admission to to the test chain is restrained the use of public condition.

The steady test structure technique permits the test chain but during the test output phase, the information is converted. In this technique, test shape is changed the use of comparator, AND gate, shift register, LFSR (Linear Feedback Shift Register).

PROPOSED METHOD

A. Authentication Block Components for tester:

The condition used for authentication through circuit under test are defined below:

Condition 1: Once the relationship among the circuit under test and authentication testers is started, the circuit under test applied a Clock sign to the testers to reach the key from the testers via Dout

Condition 2: The authentication testers gets the Clock sign and transfer the key to circuit under test

Condition 3: The circuit under test gets the key and it similarity with a previous loaded key inside the authentication

Condition 4: If the authentication is done completely, the 2nd layer of protection is turn on. Otherwise, the circuit under test transfer an authentication is not succeed and it send that message to the tester.

Step 5: The operation failed, the demo (trail) counter is increased. If the remember reaches a already defined number, the pass or fail condition is not enabled to flip blocks and its get admission to the stable experiment.
Figure. 1 Authentication Block Diagram

The authentication block diagram in Fig. 1 consists of n bit register and n bit tester input both can be given as input to the exclusive or gate and its output is applied to the n bit counter. The output of the n bit counter is applied to input of flip-flop. Flip-flop stores a single bit data and it send information to access to scan chain. With the help of trail counter is sends the information to authentication key request.

B. Scan primarily based totally attacks:

Test chains are planned to offer get entry to CUT take a look at thru check get entry to port so as to practice take a look at information to CUT all through the check condition.

The test- primarily based totally assault contains 4 workings it’s mentioned below:

i) Test-input
It is split into two levels. 1st one is to check statistics are continuous loaded into the experiment turn-flops linked to enter input. 2nd one is to the loaded facts is carried out as a take a look at the CUT.

ii) Result Observed
Circuit under test reaction is applied to the check vector and it’s covered through the test and its turn on the output connection

iii) Test –output
Shifting the observed result which is covered with the aid of using the experiment-turn to make the facts to be had output data has been tested

iv) Final Register
The application of test vector to observe the result of scan architecture. If the password is correct it move on to the next step otherwise, it again move to login window

MODIFIED METHOD

Figure. 2 Modified Method
The input(password) is fig2 given to the shift register and corresponding output is given to 2 bit counter that is given to comparator and compare the value for corresponding output and get the output in lfsr (linear shift feedback shift register). If the input(password) is wrong, then the comparator output goes to AND gate and it moves to login window(shift register)

**PROCESS1:**

![Fig3: modified method1](image)

Step1: The input (password) is given to the shift register which shifts the input values, the shifted values given to the 2 bit counter

Step2: If the password count is given as 3, it counts the value until 3, and propagate the corresponding output to the comparator

Step3: The comparator compares the corresponding output of the counter and gives the output as shown in fig3

**WAVEFORM:**

![Fig 4: process1 waveform](image)

It's compare the input and get corresponding output based on the counter value if input is same it will perform equal operation, if it is a>b it will perform greater operation as shown in fig4
A linear-feedback shift register (LFSR) is a kind of shift register its main purpose to enter bit is a linear feature of its preceding state.

The typically used linear feature of only one bits is XOR. An LFSR is a most usually a register whose enter bit is forced through the logic gates like XOR of a few bits of the general shift register value.

LFSR is works like shift register and its beginning value of the LFSR is used, due to the fact of the working of the register is predictive. The register has only limited number of possible states. It should ultimately pass into the continuous form as proven in fig5

**WAVEFORM:**

![LFSR waveform](fig6: LFSR waveform)
FINAL PROCESS:

Step1: The input (password) is given to the shift register which shifts the input values, the shifted values given to the 2 bit counter

Step2: If the password count is given as 3, it counts the value until 3, and propagate the corresponding output to the comparator

Step3: The comparator compares the corresponding output of the counter and gives the output.

Step4: The comparator output is given to the LFSR, which shifts the values as output

Step5: If the password is correct it immediately propagate the exact output, otherwise it will move to AND gate and it goes to initial stage.

The input(password) is given to the shift register and corresponding output is given to 2 bit counter that is given to comparator and compare the value for corresponding output and get the output in Lfsr (linear shift feedback shift register). If the input(password) is wrong, then the comparator output goes to AND gate and it moves to login window(shift register) as shown in fig7

WAVEFORM:

Fig7: final process

Fig8: final process waveform
CONCLUSION:

A new approach for the protection of scan architecture in opposition to the attack is presented in this paper. Security on two layers is presented. If the tester is recognized, the permission to carry out test is provided. But, critical information access is not provided in circuit under test because of second layer security. In this method is implemented by Cadence tools in CMOS 180nm technology.

REFERENCE:

[1] D. Rolt, Jean, et al. "A smart test controller for scan chains in secure circuits." 2013 IEEE 19th International On-Line Testing Symposium (IOLTS). IEEE, 2013.

[2] D. Mukhopadhyay, S. Banerjee, D. RoyChowdhury, & B. Bhattacharya, "CryptoScan: A secured scan chain architecture," 14th Asian Test Symposium (ATS’05)(pp. 348-353). IEEE. (2005, December).

[3] Y. Atobe, Y. Shi, M. Yanagisawa, & N. Togawa, "Dynamically changeable secure scan architecture against scan-based side channel attack," CUT Design Conference (ICUTC), 2012 International(pp. 155-158). IEEE (2012, November).

[4] J. Lee, M, Tehranipoor, C, Patel, and J. Plusquellic "Securing Scan Design using Lock and Key Technique," 20th international Symposium on Defect and Fault Tolerance in VLSI Systems, 2005, pp. 51-62.

[5] B. Yang, W. Kaijie, and K. Ramesh, "Secure scan: A design-for-test architecture for crypto chips," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems25, no. 10 (2006): 2287-2293.