Stream Cipher Based Encryption in IEEE Test Standards

Emanuele Valea, Marie-Lise Flottes, Giorgio Di Natale, Bruno Rouzeyre

Stream Cipher Based Encryption in IEEE Test Standards

Emanuele Valea[1], Marie-Lise Flottes[1], Giorgio Di Natale[2], Bruno Rouzeyre[1]
[1]*LIRMM (Université de Montpellier - CNRS)*, Montpellier, France
[2]*TIMA (Univ. Grenoble Alpes - CNRS - Grenoble INP*)*, Grenoble, France

***Abstract*—IEEE test standards have been developed in order to sustain the deployment of complex test infrastructures inside modern Integrated Circuits (IC). Security is a primary issue in test infrastructures. For instance, confidentiality of sensitive data flowing through the test infrastructure must be ensured. User authentication is also crucial in order to avoid secret stealing and/or device corruption. In this paper, we propose a secure JTAG implementation, based on stream cipher encryption. This countermeasure provides data confidentiality and lightweight user authentication at the cost of a little area overhead on the whole IC.**

***Index Terms*—test vs security, JTAG, scan encryption, stream cipher**

I. Introduction

The increase in complexity of modern Integrated Circuits (IC) led to the development of standard test infrastructures. These allow all the actors throughout the supply chain to perform testing, device programming, debug and diagnostics. The successive releases of the IEEE Std. 1149.1 (JTAG) [1], the IEEE Std. 1500 [2] and the IEEE Std. 1687 (IJTAG) [3] stimulated the design of hierarchical test infrastructures based on the TAP controller. As shown in Fig. 1, several scan registers are connected between the TDI and TDO pins. The Instruction Register (IR) is loaded with instructions that enable different Data Registers (DR) to be selected in the TDI/TDO serial connection. The IJTAG standard defines the rules for the integration of Reconfigurable Scan Networks (RSN) in the test infrastructure. The user can program the RSN resorting to Segment Insertion Bits (SIB), which gate embedded instruments and IP cores. Each instrument connected to the RSN offers a scan interface, called Test Data Register (TDR). In the case of embedded instruments, TDRs are simple configuration registers. Alternatively, complex IP cores give the access to their internal test infrastructure (e.g. IEEE 1500 test wrapper) through a TDR connected to the RSN of the IC.

The full deployment of standard test infrastructures can lead to security issues. Full access to the test infrastructure allows unauthorized users to perform specific attacks aimed at stealing secrets from the target IC. Moreover, IP cores connected to the test infrastructure have access to all test data shifted through the scan network. Hence, malicious IP cores can be a threat if they hide functionalities, that allow them to perform sniffing of test data and/or tampering with their content [4].

*Institute of Engineering Univ. Grenoble Alpes

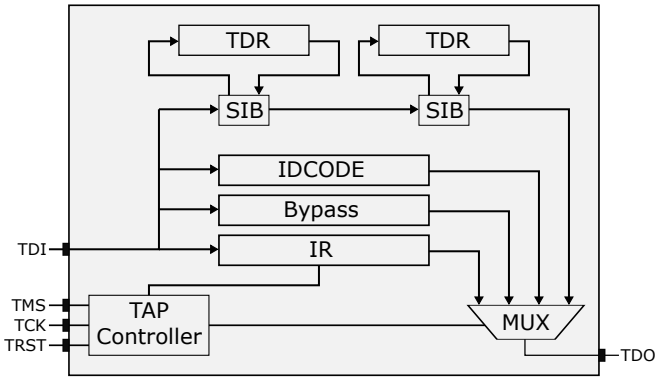

Fig. 1. Example of standard test infrastructure.

Test data encryption has been proposed in order to provide data confidentiality inside the test infrastructure [5]. Test data are encrypted when shifted through the scan network, so that malicious entities cannot sniff their content. Illegal access to the test infrastructure and data tampering are also made too complex. In fact, lightweight user authentication is also granted by the scan encryption technique.

In this paper, we present a modified implementation of the JTAG TAP controller, which favors the integration of the encryption in standard test infrastructures resorting to the stream cipher.

II. Scan Encryption with Stream Cipher

Scan encryption schemes rely on symmetric ciphers, because of their smaller footprint. These ciphers are based on a secret key that is shared between the user and the device. On the device side, the key is stored in a secure memory and it is only known by authorized users. If different IP cores in the same IC are equipped with scan encryption, each of them must have a secret key secured in the IC.

Each IP core has a decryption module at the TDI pin and an encryption module at the TDO pin. The user must send test data encrypted using the shared secret key. Encrypted data are decrypted as soon as they reach the TDI pin of the target IP core. Untrusted IP cores that are traversed by the same scan network, receive encrypted data. Thus, it is impossible for them to retrieve any information. Before responses are shifted out the TDO pin, they are encrypted by the encryption module. As a consequence, IP cores that are placed downstream along the scan network, also receive encrypted data. At the end,

the user decrypts the responses and obtains the confidential information.

The stream cipher is a symmetric encryption scheme that perfectly fits the serial interface of scan networks. The input bitstream, containing the plaintext message, is XORed with a pseudo-random keystream. The keystream is generated by a Pseudo-Random Generator (PRG), such as the *Trivium* stream cipher. The Trivium stream cipher is based on a non-linear LFSR, which is seeded with an 80-bit secret key and an 80-bit Initialization Vector (IV). While the secret key is fixed and permanently stored inside the device, the IV must change at every encryption session for security reasons (e.g. *two-times pad* attack). In fact, the same keystream must never be used to encrypt more than one plaintext message.

III. Encrypted Test Infrastructure

The proposed test infrastructure relies on a modified TAP controller. The basic idea is to divide data registers in two categories: *protected* and *non-protected*. As is shown in Fig. 2, protected DRs are connected to a separate branch of the test infrastructure, where data shifted through the TDI and TDO pins passes through the stream encryption/decryption process. The IR is always non-protected, because JTAG instructions are always publicly known. If the user wants to execute an instruction that selects a protected DR, he or she is obliged to start setting an encrypted communication in order to be able to load data into the corresponding DR.

A new JTAG instruction, called *GETIV*, is implemented, in order to request a fresh IV from the device. This is internally generated and stored inside a special non-protected DR. The generated IV is shifted out through the TDO pin as a response to the *GETIV* instruction. At this point, the user relies on the new IV and the secret key, in order to send properly encrypted data and to correctly decrypt the responses.

The device must always generate a different IV after each reset of the circuit. For this reason, a True Random Number Generator (TRNG) can be used. TRNGs are characterized by a high implementation cost. However, modern ICs with security functions are equipped with at least one TRNG. This can be shared with the test infrastructure in order to hand out IVs under request. For this reason, we do not consider the TRNG cost as part of the implementation overhead of the proposed solution.

Once test data are decrypted, they are shifted through the DRs as plaintext. In the case in which an IJTAG RSN is present inside the test infrastructure, IP cores with their own TAP interface can be part of the network. In this case, each IP core can implement the same technique on its proper test infrastructure. This way, only specifically authorized users can execute protected instructions on the IP core's TAP controller.

The encrypted test infrastructure grants the confidentiality of data that are exchanged between the target device and the user. Moreover, unauthorized users cannot successfully execute protected instructions on the target test infrastructure, because any data inserted in the protected DRs are unpredictably decrypted at the TDI pin.

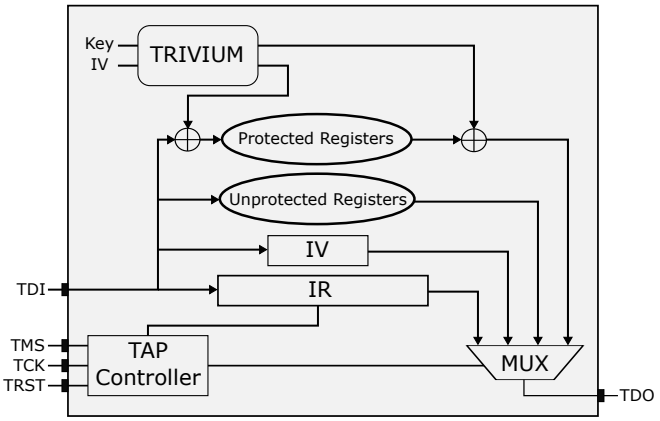

Fig. 2. Test infrastructure with scan encryption.

At first glance, the area overhead seems to be very large, as shown in Tab. I. Nevertheless, compared to the whole area of a modern IC, this overhead is negligible. For instance, this countermeasure on a LEON3 microprocessor leads to an area overhead of merely 0.41%.

TABLE I
Area Overhead Evaluation

Modules	Original JTAG (GEs)	Encrypted JTAG (GEs)
JTAG wrapper	625	1147
TRIVIUM	/	2048
IV Shift Register	/	300
Control Unit	/	252
Total	***625***	***3747***

IV. Conclusions

Modern test infrastructures lack of lightweight confidentiality and user authentication mechanisms. We have proposed a modified JTAG controller, which supports the encryption of a set of protected JTAG instructions. The present technique can be easily extended to all hierarchy levels of a modern IC test infrastructure.

References

[1] R. of IEEE Std 1149.1-2001, "IEEE standard for test access port and boundary-scan architecture," *IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001)*, pp. 1–444, May 2013.

[2] R. of IEEE Std 1512.1-2003, "IEEE standard testability method for embedded core-based integrated circuits," *IEEE Std 1500-2005*, 2005.

[3] "IEEE standard for access and control of instrumentation embedded within a semiconductor device," *IEEE Std 1687-2014*, pp. 1–283, Dec 2014.

[4] E. Valea, M. Da Silva, G. Di Natale, M. Flottes, and B. Rouzeyre, "A survey on security threats and countermeasures in IEEE test standards," *IEEE Design & Test*, pp. 1–1, 2019.

[5] E. Valea, M. D. Silva, M.-L. Flottes, G. D. Natale, and B. Rouzeyre, "Stream vs block ciphers for scan encryption," *Microelectronics Journal*, vol. 86, pp. 65 – 76, 2019.