Secure Test with RSNs: Seamless Authenticated Extended Confidentiality

Paolo Maistri, V. Reynaud, Michele Portolan, Régis Leveugle

Secure Test with RSNs:

Seamless Authenticated Extended Confidentiality

P. Maistri, V. Reynaud, M. Portolan, R. Leveugle
Univ Grenoble Alpes, CNRS, Grenoble INP[1], TIMA, 38000 Grenoble, France
{firstname.lastname}@univ-grenoble-alpes.fr

Abstract— **The testability of electronic devices is of critical importance and it is often supported by IEEE standards. The presence of test structures, on the other hand, paves the way for malicious attackers to access the circuit and extract confidential knowledge such as secret keys or intellectual property. Removing the access to these structures after manufacturing test may prevent security breaches, but this solution is not definitive and excludes the possibility of advanced uses such as online debugging, diagnosis of designs and on-line updates or monitoring. For this reason, it is important to maintain the test infrastructure but to protect it against threats either external (e.g., attackers) or internal (e.g., hardware trojans). This can be achieved through protocols ensuring authentication added to confidentiality capabilities. In the case of Reconfigurable Scan Networks (RSN - IEEE 1687), some solutions currently exist, but are limited to external threats. In this paper, we review the recent state of the art in the domain, and present a novel solution addressing in a comprehensive and low-cost manner authentication and confidentiality, both inside and outside the device.**

Keywords— Secure test, confidentiality, authentication, RSN, IEEE 1687, SIB

I. Introduction

Testing the correct behavior of digital circuits after their fabrication has always been a critical challenge for designers and developers of CAD tools. Over time, the push for efficient and cost-effective techniques to diagnose and debug, even during device's lifetime, has led to the definition of standard architectures and protocols to guarantee interoperability. Standards such as IEEE 1149.1 [1] and IEEE 1500 [2] were thus introduced, aiming to increase test performance, observability, and controllability. As the complexity of designs and of Systems-on-Chips (SoCs) increased, existing standards needed evolving and the addition of features aimed at reducing such complexity. Recently, IEEE 1687 [3] has introduced the dynamic reconfiguration of the scan chain: the scan structure can be organized into subsections, which can be included or excluded at test time to focus the test procedure on specific regions of the design thanks to structures such as the Segment Insertion Bits (SIBs).

On the other hand, it is nowadays well-known that these facilities may be a dangerous entry point into the circuit, and can be exploited by malicious third-parties [4]-[6]. Potential threats can materialize as sensitive data leakage [7], device tampering to induce improper behavior [8], or theft of Intellectual Properties (IPs) [9].

Among the different solutions related to the vulnerabilities and security of the test infrastructure, a large effort has been recently dedicated to (1) limit the access to the internal regions of the system only to authorized users, and (2) prevent information leakage through test data. So far, the usual threat model has been the external attacker, who may intercept the communication between the device and the test equipment. This is the reason why these two issues have been mostly considered and addressed separately: existing works deal either with scan network access authentication, or with encryption to guarantee confidentiality outside the device.

More recently, with the increasing complexity of systems and the proliferation of subcontracting, this model was found to be no longer fully representative. Internal threats need to be considered as well: embedded IPs, not developed in-house, cannot be considered trustable if a sensitive application is envisioned, and proper actions must be taken to ensure correct and efficient testing under these circumstances. Malicious IPs might monitor and exploit the data transiting in the scan chain in order to extract useful knowledge.

With this work, we aim at summarizing most recent advances in the field, identify the common elements, and propose a merging step where both authentication and encryption can coexist effectively and where both external and internal threats can be addressed with limited or negligible impact on test performance.

The paper is organized as follows. In the next section, the state of the art concerning authentication mechanisms to access the scan chain and techniques for the confidentiality of the test vectors is presented. Section III presents our novel proposal aimed at improving the granularity of the confidentiality in the scan chain and based on an Encryption SIB (eSIB). Finally, Section IV concludes the paper.

II. Security in the Scan Network: a State of the Art

A. Secure Access and Authentication

The access management goal starts from the assumption that the authorized user has an information token (i.e., the key) granting him access rights to the corresponding part of the circuit. In order to limit the complexity of the implementation, distributed schemes can be employed: the Locking SIB [10], for instance, is a special SIB that is unlocked only when a specific condition on a certain number of bits, distributed and hidden within the scan chain, is met. This method allows a fine resolution in access management, but the protocol is not safe as the key is transferred plainly and if an attacker intercepts that data, a simple replay attack allows unlocking the system.

More secure protocols need the key not to be exchanged in clear format, which usually means resorting to some

[1] Institute of Engineering Univ. Grenoble Alpes

cryptographic function: symmetric [11], asymmetric [12], or hashing primitives [13]. However, in these works the critical issue remains the fact that the distribution of credentials is plainly done over the scan chain, which is not desirable.

For this reason, the use of a Challenge/Response protocol has been recently proposed: though more complex, it ensures better security with respect to the previous solutions. In [14], the authors combine the challenge-response scheme with the use of a second scan chain (the Secure Scan Chain, SSC) to distribute the opening authorizations. The protected SIBs are called Secure SIBs (S²IB, shown in Figure 1) and can include only subparts of the network, which can be unlocked if an authorization is delivered through the SSC. A controller drives the secure chain and communicates with the user through a segment of the main scan chain. The proposed scheme is strong, but requires a separate key for each different instrument: in large SoCs, this increases the authentication latency and the hardware cost to embed all the keys. It is also difficult to make the keys flexible, either to personalize the circuits or to update the authorizations during lifetime. For this reason, in [15] the authors propose to generate the keys procedurally from a unique circuit key and a configuration vector: several instruments can be accessed in parallel if the corresponding authorizations are granted, thus speeding up the authentication latency and the cost of key storage.

B. *Confidentiality of Vectors: A Global Approach*

As discussed previously, attacks to the scan infrastructure can extract confidential information by reverse engineering the structure of the scan network itself through differential analysis of several input vectors [4],[6]. The intelligibility of the data extracted from the scan chain is thus a basic requirement for the attack to succeed.

For this reason, one of the first countermeasures proposed in the literature was based on scrambling the scan chain [16]. The network is split into several segments, that are reordered according to a secret key, embedded into the device and known only by the authorized testers. Without knowing the correct key, the scan flip-flops are randomly arranged and the attacker is not able to extract the information, while the testability of the device is preserved.

Another approach based on obfuscation is presented in [17], where the plain scan chain is obfuscated through additional XOR gates within the scan cells, and then masked by an obfuscation key generated by an LFSR. The security of the mechanism is based on the fact that only the IC designer knows the obfuscation scheme, the LFSR initialization, and the key update frequency.

Other recent approaches are based on the encryption of test vectors: once generated, the input patterns are encrypted offline and sent through the test input port into the circuit, where they are decrypted and used. Likewise, outputs are encrypted within the device and sent through the test output port and decrypted offline, where they can be analyzed for debugging. Any symmetric primitive can be used for encryption/decryption: block ciphers [18][19] are secure, but they need proper padding management if the scan length is not a multiple of the block size, and managing the dynamic structure of RSNs can be complex.

For this reason, stream ciphers have been proposed. These primitives can produce an encrypted output of indefinite length, starting from a secret key and a public initialization

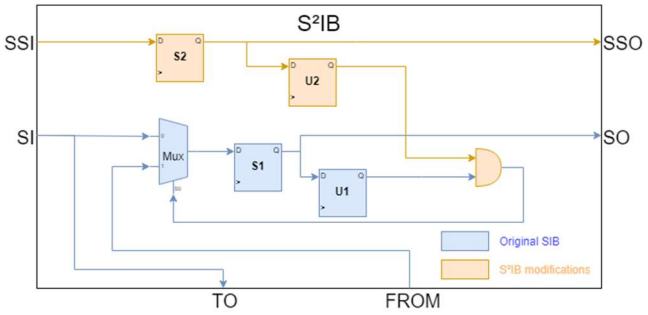

Fig. 1. Architecture of the Secure SIB (S²IB)

Vector (IV). In [9], the stream cipher is proposed to protect the communication through the JTAG interface: the secret key is provided by the user (as a challenge value) whereas the IV is hardwired into the device at fabrication; then, the first output bits of the stream ciphers are used back as secret key for the actual ciphered stream. The same authors have later proposed a similar scheme to directly encrypt the test vectors [20] within the IEEE 1500 standard: the secret key is directly provided by the user and fed through a dedicated channel, not shared with other (potentially insecure) IPs. In [21], the authors propose again the use of stream ciphers to protect the scan network: however, they do not give any detail concerning the IV generation, whereas the secret key is embedded through fuses or through a PUF, whose output must be registered at fabrication.

The use of a stream cipher is confirmed in [22], where the secret key is provided by the user, whereas the IV is generated internally using a True Random Number Generator. This approach ensures that the scheme is robust enough against attacks based on value reuse or collisions. The authors propose to extend the JTAG instruction set in order to read the IV value from the circuit. As this value is not controllable by the user and is valid only for the current session, the protocol cannot be broken by replay attacks.

III. SEAMLESS INTEGRATED SECURITY

As we have seen so far, solutions from the state of the art already provide some protections against malicious attacks. Access authentication protects from external threats, while scan encryption protects against spoofing. The latter protects the observability of the circuit, whereas the former secures also its controllability avoiding potential harmful accesses. They are complementary and can be effectively combined; additionally, sharing the same cryptographic core gives significant savings in resources.

A. *Confidentiality per IP*

With respect to the confidentiality schemes existing in the state of the art, however, current implementations suffer from some limitations. Initial solutions were based on the confidentiality provided by obfuscation, but once this veil is removed, the design becomes exposed. Protocols based on symmetric ciphers, on the other hand, rely on well-known algorithms that can guarantee strong security. In the state of the art, however, the encryption/decryption layer is applied at the level of the test controller: as a consequence, the full scan chain is encrypted when the secure exchange is enabled. This protects against external and internal spoofing: data is unintelligible by the attacker, or by any internal malicious IP, without the decryption key. On the other hand, it affects the test procedures, as it implies that when a secure element is accessed, all the rest of the scan chain cannot be used, as the

content of the flip flops would be encrypted and thus useless for debugging. Moreover, if several secure instruments exist in the scan chain but they do not share the same key (for instance, because they come from different providers), they will need to be accessed separately even if the user has the proper access privileges for both.

In order to maximize the effectiveness and the performance of the scan network while preserving at the same time the security of the system, data should be secured at the segment level. This means that for each sensitive instrument, the test values should be decrypted only when entering the corresponding segment, and re-encrypted at the output. In this case, however, employing a dedicated cryptographic IP for each segment would incur costs that would be excessive for a test infrastructure.

On the other hand, if the cryptographic unit was centralized, the additional hardware in each SIB would be kept to a minimum and the overall impact reduced. This can be achieved, for instance, by masking the test vectors with the output of a stream cipher, as proposed in previous solutions: with this approach, the only additional hardware required is the XOR gates used to decrypt (unmask) and re-encrypt (mask) the test values.

The difficulty, in this case, resides in the distribution of the key stream over the scan network. We propose to solve this issue by reusing and extending the Secure SIB elements already used in authentication protocols such as FGA or SSAK. The Secure Scan Chain can be therefore reused to distribute the stream coming from the centralized cipher and feed the masking logic. The new Encryption SIB, shown in Figure 2, can therefore guarantee secure access control through the chosen authentication protocol, and also confidentiality with a very limited overhead: the only additional cost consists of two XOR gates for each Secure SIB attached to a sensitive segment. Figure 3 shows the cost of implementing different authenticated access schemes: LSIB is the least expensive but also the least secure; FGA is slightly more expensive, due to the larger key memory, while the incremental cost of eSIBs with respect to SSAK is negligible. It is interesting to note that the cost of schemes other than LSIB depends heavily on the chosen cryptographic primitive: if a lightweight cipher is used, e.g. Grain, then FGA, SSAK, and eSIB are suitable from as low as 10 protected SIBs.

Such a low overhead in the SIB is possible thanks to the choice of reusing the SSC, whose purpose is now twofold: distribute the access authorization data for the secure segments, or distribute the key stream coming from the centralized cryptographic unit, which can be shared with the authentication protocol as well. In order to discriminate between the two different transiting data streams, an arbiter must be used at the root of the SSC, which will propagate the correct information at the right time, as shown in Figure 4. The advantage is clear when considering the much lower complexity in routing: a dedicated path for the key stream would hugely increase the connectivity complexity of nodes in the circuit, and strongly impact the achievable density and/or performance.

B. *Discussion*

The presented solution puts together the hardware structures used for authentication and confidentiality and merges them in the Encryption SIB, making it much simpler to integrate both protocols at the same time. Its simplicity,

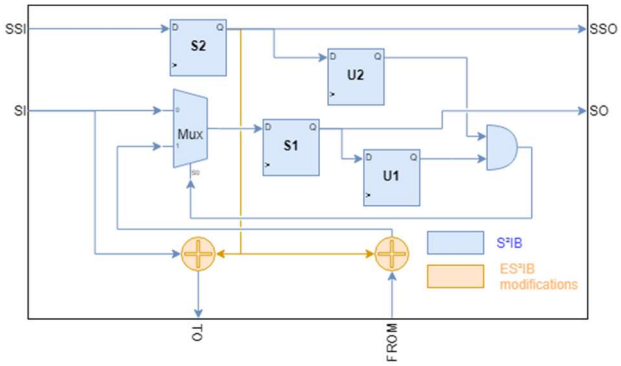

Fig. 2. Architecture of the Encryption SIB (eSIB).

however, leaves nonetheless the designer with a non-negligible issue: the alignment of the key stream. If we use a dedicated cipher for each bit, the cost increases but we can be sure that the key stream perfectly fits to the segment it belongs to; this, on the other hand, is not so simple if the cryptographic core is centralized. In this case, the fact that the key addition is within the scan chain, and not at its boundaries as in [22], causes a phase shift between the data and the key. If a stream cipher is used, then the phase shift can be easily corrected by a corresponding shift in the key stream provided by the user. Additionally, it is important to stress the fact that the reconfiguration of the RSN can modify this phase shift, even by adding or removing encryption points in the scan chain.

For each (un)masking (XOR) gate, two different phase shifts, for reading and writing, need to be computed. The exact phase shifts can be computed as follows. If we consider:

- n the length of the Secure Scan Chain (SSC),
- m the length of the chain before the XOR gate,
- o the length of the chain after the XOR gate,

we can then compute the key phase shifts ϕ_i (for the scan input) and ϕ_o (for the scan output) as

$$\phi_i = n - m, \text{ and}$$
$$\phi_o = n + o$$

where the intermediate steps were omitted for readability. Hence, when scanning in the test vector, the corresponding key stream must be preprocessed off-chip and delayed by the difference between the length of the SSC and the length of the segment of the scan chain before the unmasking XOR gate. On the other hand, when scanning out, the key stream must be advanced by the SSC length and by the size of the scan chain after the masking XOR gate.

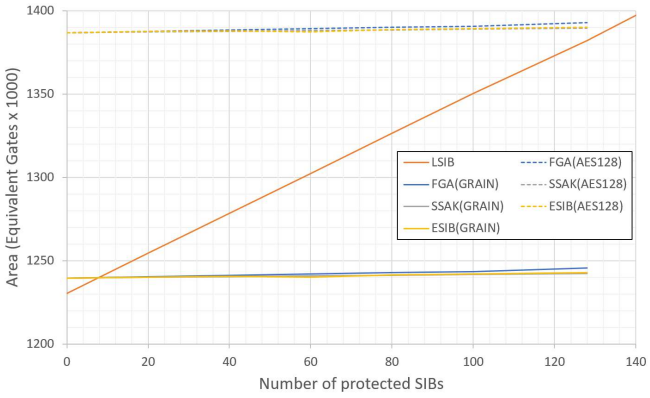

Fig. 3. Comparative costs of Scan Chain Authentication Protocols when using AES-128 or Grain: SSAK and eSIB overlap (AMS c35, Equivalent Gates)

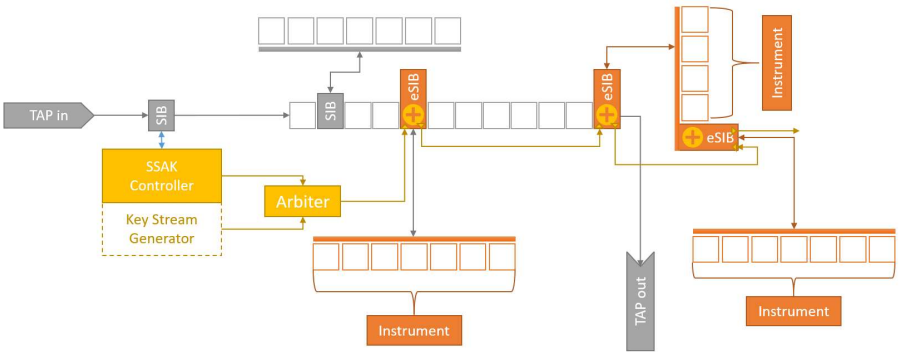

Fig. 4. Key distribution in the protected scan chain

Thanks to the linear properties of the XOR operation, several segments can be protected at the same time, provided that the correct pre-processing for the key stream is computed for each segment. Moreover, we suggest to combine per-segment encryption with global scan chain encryption, as presented in recent SoA. It must be pointed out, however, that the scan chain lengths are not necessarily constants due to their reconfigurability. The user must hence be able to know the effective length of the scan chain at all times, in order to adapt the phase shifts of the encryption keys.

IV. Conclusion

Testing and Security are no longer mutually exclusive. Recent standards allow for confidentiality or secure access for the scan infrastructure. In this paper, we have proposed the eSIB, a novel solution integrating both requirements in the same structure at negligible cost. The main issue is the proper key alignment, a problem that will be addressed in the future by resorting to modern Test Management Tools.

Acknowledgment

This work has been partly funded by the French Government under the framework of the PENTA HADES ("Hierarchy-Aware and secure embedded test infrastructure for Dependability and performance Enhancement of integrated Systems") European project.

References

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

[2] IEEE std 1500 - Standard for Embedded Core Test - http://grouper.ieee.org/groups/1500/.

[3] IEEE Std 1687-2014, "IEEE Standard for Access and Control of Instrumentation Embedded within a Semiconductor Device", IEEE, USA, 2014

[4] Bo Yang, Kaijie Wu and Ramesh Karri, "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard," 2004 International Conference on Test, Charlotte, NC, USA, 2004, pp. 339-344, doi: 10.1109/TEST.2004.1386969.

[5] X. Li, W. Li, J. Ye, H. Li and Y. Hu, "Scan Chain Based Attacks and Countermeasures: A Survey," in IEEE Access, vol. 7, pp. 85055-85065, 2019, doi: 10.1109/ACCESS.2019.2925237.

[6] D. Ray, S. Singh, S. S. Ali and S. Biswas, "Co-relation Scan Attack Analysis (COSAA) on AES: A Comprehensive Approach," 2019 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Noordwijk, Netherlands, 2019, pp. 1-6, doi: 10.1109/DFT.2019.8875272.

[7] Sk Ali, Samah Saeed, Ozgur Sinanoglu, Ramesh Karri. New Scan-Based Attack Using Only the Test Mode and an Input Corruption Countermeasure. 21th IFIP/IEEE International Conference on Very Large Scale Integration - System on a Chip (VLSI-SoC), Oct 2013, Istanbul, Turkey. pp.48-68, ff10.1007/978-3-319-23799-2_3ff.

[8] Mark Barnes, "Alexa, are you listening?", MWR Info Security, https://labs.mwrinfosecurity.com/blog/alexa-are-you-listening/, Aug 1st 2017.

[9] K. Rosenfeld and R. Karri, "Attacks and Defenses for JTAG," in IEEE Design & Test of Computers, vol. 27, no. 1, pp. 36-47, Jan.-Feb. 2010.

[10] Jennifer Dworak, Al Crouch, John Potter, Adam Zygmontowicz, Micah Thornton, «Don't Forget to Lock your SIB: Hiding Instruments using P1687», IEEE International Test Conference, 2013.

[11] M. Aigner and M. Feldhofer, "Secure Symmetric Authentication for RFID Tags," in Telecommunication and Mobile Computing, 2005.

[12] J. Da Rolt, S. Ghosh, S. Seys, S. Dupuis, G. Di Natale, L. Marie-Flottes, B. Rouzeyre and I. Verbauwhede, "Secure JTAG implementation using Schnorr protocol," Journal of Electronic Testing, vol. 29, pp. 193-209, 2013.

[13] E. Koopahi and S. E. Borujeni, "Secure scan-based design using Blum Blum Shub algorithm," in East-West Design & Test Symposium (EWDTS), 2016.

[14] B. Rafal, K. Michael A and H.-J. Wunderlich, "Fine-Grained Access Management in Reconfigurable Scan Networks," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, pp. 934-947, 2015.

[15] M. Merandat,, V. Reynaud, E. Valea, J. Quevremont, N. Valette, P. Maistri, R. Leveugle, M.-L. Flottes, S. Dupuis, B. Rouzeyre, G. Di Natale, "A Comprehensive Approach to a Trusted Test Infrastructure," in Internation Verification and Security Whrokshop, Rhodes 2019.

[16] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, N. Berard, et al.. Scan design and secure chip [secure IC testing]. IOLTS: International On-Line Testing Symposium, Jul 2004, Madeira Island, Portugal. pp.219-224, DOI: 10.1109/OLT.2004.1319691.

[17] X. Wang, D. Zhang, M. He, D. Su and M. Tehranipoor, "Secure Scan and Test Using Obfuscation Throughout Supply Chain," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 9, pp. 1867-1880, Sept. 2018.

[18] M. Da Silva, M. Flottes, G. Di Natale, B. Rouzeyre, P. Prinetto and M. Restifo, "Scan chain encryption for the test, diagnosis and debug of secure circuits," 2017 22nd IEEE European Test Symposium (ETS), Limassol, 2017, pp. 1-6, doi: 10.1109/ETS.2017.7968248.

[19] M. Da Silva, M. Flottes, G. Di Natale and B. Rouzeyre, "Preventing Scan Attacks on Secure Circuits Through Scan Chain Encryption," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 38, no. 3, pp. 538-550, March 2019, doi: 10.1109/TCAD.2018.2818722.

[20] K. Rosenfeld and R. Karri, "Security-aware SoC test access mechanisms," 29th VLSI Test Symposium, Dana Point, CA, 2011, pp. 100-104.

[21] S. Kan, J. Dworak and J. G. Dunham, "Echeloned IJTAG data protection," 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST), Yilan, 2016, pp. 1-6.

[22] E. Valea, M. da Silva, M.-L. Flottes, G. Di Natale, B. Rouzeyre. Encryption-Based Secure JTAG. DDECS: Design and Diagnostics of Electronic Circuits Systems, Apr 2019, Cluj-Napoca, Romania. DOI: f10.1109/DDECS.2019.8724654.