Active Shield with Electrically Configurable Interconnections

Umut Guvenc
National Research Institute of Electronics and Cryptology
BILGEM TUBITAK
Kocaeli, Turkey
e-mail: umut.guvenc@tubitak.gov.tr

***Abstract*—An active shielding method is hereby introduced, providing security to security critical integrated circuits against some physical attacks such as probing, manipulation and modification. Active shields satisfy a physical clearance by preventing the reachability of the circuitry while they, themselves, are subject to modification in most cases. The proposed active shield, which is also subject to a patent application, provides the ability to detect any physical modification made on the shield itself by utilizing electrically configurable interconnections between shielding metal lines. By changing the selected interconnection configuration of the shielding lines, the proposed active shield provides a self detection ability as a countermeasure against the vulnerability to physical modification made on the active shield itself.**

Keywords-active shield; secure IC; cryptography; physical attack countermeasure

I. INTRODUCTION

In security critical integrated circuits, some security countermeasures are implemented to provide safety of the critical information against some analysis and attack techniques. Some of these attack techniques aimed to obtain the information in an unauthorized way are known as physical attacks since they require actual physical access to the inner layers of the integrated circuit. Upon this attack concept, one should try to obtain the secret information via probing, manipulation or modification. These attack techniques include probing the critical information by making connections to the metal lines of the integrated circuit, faulting the integrated circuit by forcing from these outside connections and changing the connections of the internal metal lines permanently by using Focused Ion Beam (FIB) [1]. Active shield [2] is a countermeasure against these kinds of attacks, to be applied to the security critical integrated circuits which are physically accessible.

In active shield method, the whole surface of the integrated circuit is covered by metal lines on the top metal layer. These metal lines are supplied with a predefined or random test data from a transmitter and observed with a number of receivers located at certain points of the integrated circuit. The receivers are also supplied with the same test data internally thus they can compare the data on the shielding metals and the actual test data. According to the result of the comparison, these receiver circuitries verify the integrity of the top layer metal lines. Since any physical attack will disturb the integrity of these shielding lines by making them open or short circuit, the receiver circuitries do not receive the correct test data pattern from the shield, thus detect the physical attack.

It is believed that [3], [4], [5], [6] and [7] provide sufficient information on the background of the active shield method. In [3], a way of implementing the active shield method without requiring an additional metal layer is introduced, and in [4] [5], improvements are aimed to reduce the power consumption due to active shield. Derouet [6] introduced some improvements mainly on the detection circuitry part of the active shield method, not on the protection of the top metal layer shield itself.

Although being used in integrated circuits to detect any physical attack, active shield itself has still vulnerability against physical modification. Since the top layer metal lines of the active shield have fixed interconnections, it is possible to make shortcut connections between the lines and remove the parts covering the whole integrated circuit or a part of it, to perform the actual attack without being detected by the active shield. Some improvements can be made to decrease the vulnerability of the active shield to physical modification, like randomization of the connections of the top layer metal lines and increasing the number of receiver circuitries, however it is not possible to prevent the vulnerability completely.

In [7], a novel countermeasure against physical modification on the active shield is introduced. A capacitive measurement between the top layer metal lines of the active shield is performed along with the verification of the test data, to check whether the top layer metal lines are integral in their actual shapes. However, since the mentioned capacitive measurement between the top layer metal lines cannot be performed precisely, it is still possible for an attacker to perform partial physical modifications on the active shield while still satisfying sufficient capacitive coupling between the top layer metal lines.

In this work, an active shield aimed to prevent the vulnerability caused by the fixed interconnections of the shielding metal lines, by introducing a method using electrically configurable interconnections is proposed. Using electrically configurable interconnections provides the opportunity to select from more than one interconnection scheme during the operation of the integrated circuit. This dynamic configurability introduces a precise self-integrity checking mechanism to the active shield method. Thus, it is

 ISBN: 978-1-61208-298-1

prevented to bypass and remove the metal lines of the active shield by making fixed shortcut connections between them.

II. IMPLEMENTATION

A regular active shield implementation is shown in Fig. 1. In this implementation, the whole surface of the integrated circuit is covered by parallel shielding metals which are connected randomly yet fixed interconnections to each other to form the bit lines carrying the test data. The transmitter, receivers and the internal data paths between them are supposed to be hidden in the other circuitry thus cannot be recognized. The receiver circuitries verify the integrity of the shield by comparing the data received from the shielding lines with the actual data received internally. However, one should attempt to uncover the security critical circuit by making some external shortcut connections between the lines of the active shield as illustrated in Fig. 2. In such a case, the active shield would still claim that the shield is integral. By increasing the number of bit lines and the number of receivers, forming shortcut connections can become harder; however, the vulnerability is not prevented completely.

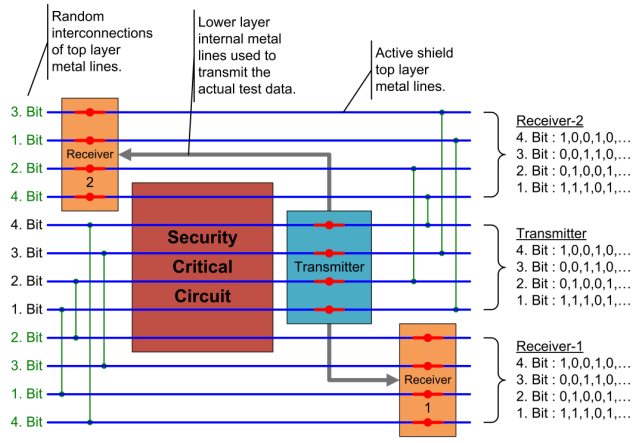

Figure 1. A regular active shield implementation with fixed interconnections.

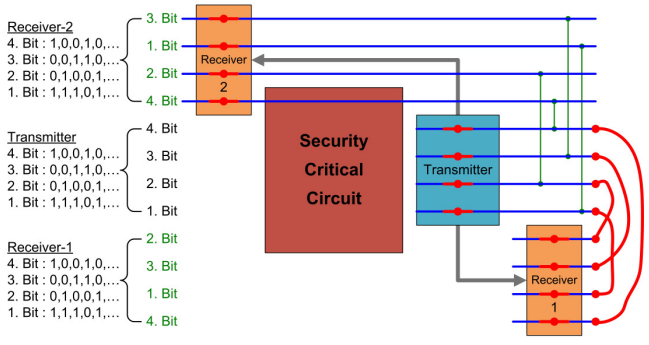

Figure 2. Illustration of bypassing the regular active shield.

In Fig. 3, an implementation of the proposed active shield is shown. The top layer metal lines are arranged in the same manner to cover the whole surface of the integrated circuit. Interconnections between the parallel metal lines are realized by using electrically switching circuits selecting from different random interconnection configurations. In the embodiment shown in Fig. 3, two different interconnection configurations are realized with switching circuits, which are in fact sufficient for the purpose of the active shield. The transmitter transmits a test data along with a select signal used to determine which interconnection configuration is selected. The receivers receive the test data from the bit lines and reorder the bits of the data received according to the select signal produced by the transmitter. The receivers also receive the same test data from the transmitter through internal data buses. The receivers verify the integrity of top metal lines of the active shield by comparing the test data received from the bit lines with the actual test data received from the internal data buses. Generally, the internal data buses carrying the actual test data the select signal, and the transmitter and the receivers themselves are arranged as a part of the integrated circuit such as distributed within the whole layout and not easily recognizable for the sake of security. Thanks to the electrically controllable switching circuits used to construct different interconnection configurations, the proposed active shield verifies the test data received from the bit lines with the actual test data for detection of the physical attacks focused on the integrated circuit, while providing the ability to detect any fixed modification made to bypass the shielding pattern and remove at least a part of it. In order to satisfy the latter purpose, the transmitter changes the selected interconnection configuration during the operation of the integrated circuit by changing the select signal regularly or randomly. Thus, any fixed physical modification on the upper layer conductive lines leads to an error in the verification of the test data.

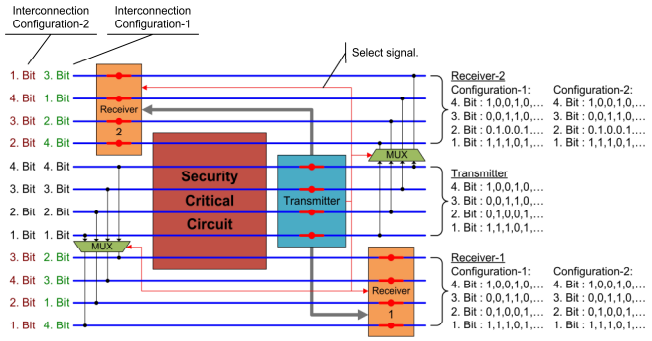

Figure 3. Proposed active shield implementation with electrically configurable interconnections.

Fig. 4 illustrates a bypassing attack on the proposed active shield. In the illustration, shielding metal lines are partly removed from the top of the security critical circuit by making fixed shortcut connections. These shortcut connections between the transmitter and one of the receivers are arranged to preserve the integrity of the bit lines according to the first interconnection configuration. Although the fixed shortcut connections satisfy the correct transmission of the test data when the first interconnection

 ISBN: 978-1-61208-298-1

configuration is selected, they do not satisfy the correct transmission of the test data when the second interconnection configuration is selected. Since the transmitter changes the select signal during the operation of the integrated circuit, the receivers would test the integrity of the shielding metal lines for all of the interconnection configurations and detect the attack. Thus, the vulnerability of the active shield to physical modification is prevented.

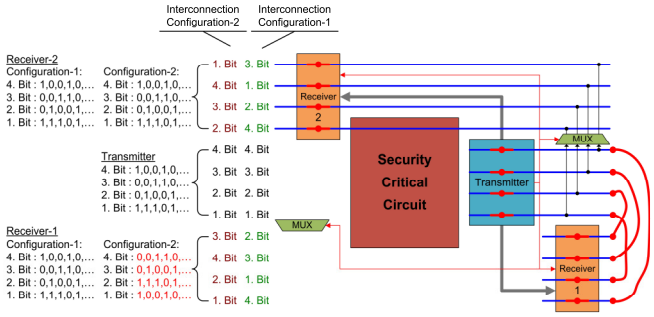

Figure 4. Illustration of bypass connections made on the proposed active shield and the detection of the modification.

Fig. 5 shows an exemplary embodiment of the electrically controllable switching circuits. Four two-input multiplexers are used to construct a part of the two different interconnection configurations of four bit lines as an example. The select signal determines in which order the inputs of the multiplexers are connected to the outputs.

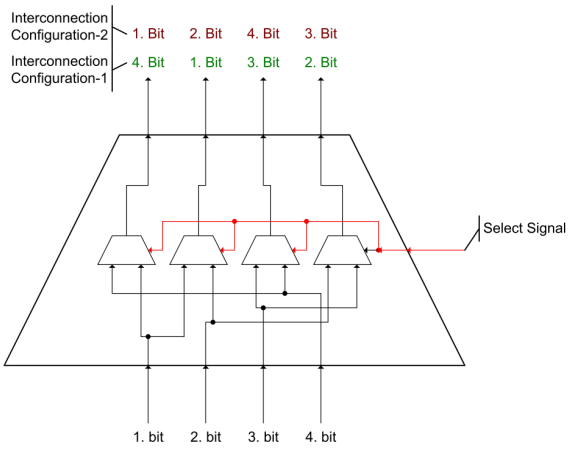

Figure 5. Exemplary embodiment of the electrically controllable switching circuits.

As seen in Fig. 5, electrically controllable switching circuits can be realized easily within a digital design, since they consist of basic multiplexer standard cells. The realization and the placement of multiplicity of these circuitries can be done by even automatic place and route approach or some scripting in the layout generation step.

III. CONCLUSION

A novel active shielding method is proposed, which has the ability to detect any bypassing attempt made by fixed physical modifications. Electrically controllable switching circuits are used to construct dynamically selectable different interconnections schemes between shielding metal lines.

ACKNOWLEDGMENT

The proposed active shield method is subject to a patent application numbered as 2011/11432 by Turkish Patent Institute.

REFERENCES

[1] M. Witteman, “Advances in smartcard security”, Information Security Bulletin 7.2002: 11-22.

[2] S. Briais, et al. “Random Active Shield”, Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on. IEEE, 2012.

[3] A. Beit-Grogger and J. Riegebauer, “Integrated circuit having an active shield”, US Patent 92848 A1, published in May 5, 2005.

[4] G. Cutrignelli and R. Malzahn, “Circuit Arrangement, data processing device comprising such circuit arrangement as well as method for identifying an attack on such circuit arrangement”, US Patent 24890 A1, published in January 22, 2009.

[5] J. Ziomek, “Method to reduce power in active shield circuits that use complementary traces”, US Patent 150574 A1, published in January 26, 2008.

[6] O. Derouet, “Integrated circuits including reverse engineering detection using differences in signals”, US Patent 244749 A1, published in October 2, 2008.

[7] P. Laackmann and H. Taddiken, “Apparatus for protecting an integrated circuit formed in a substrate and method for protecting the circuit against reverse engineering”, US Patent 132777 A1, published in July 17, 2003.

 ISBN: 978-1-61208-298-1