COMPUTERS & SECURITY XXX (XXXX) XXX

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Random active shield generation based on modified artificial fish-swarm algorithm

Ruishan Xin[a,b], Yidong Yuan[a,b], Jiaji He[a,b], Shuai Zhen[a,b], Yiqiang Zhao[a,b,*]

[a] School of Microelectronics, Tianjin University, Tianjin 300072, China
[b] Tianjin Key Laboratory of Imaging and Sensing Microelectronic Technology, Tianjin 300072, China

ARTICLE INFO

Article history:
Received 13 November 2018
Revised 8 April 2019
Accepted 8 June 2019

Keywords:
Integrated circuits
Invasive attacks
Active shield
Random Hamiltonian path
Artificial fish-swarm algorithm

ABSTRACT

Active shield has already been a primitive sensor of security critical integrated circuits for detecting invasive attacks. Because of the complex topology structure, the active shield based on random Hamiltonian path has a high security level. However, the available generation algorithms of this random path have poor efficiency when shield area is large, restricting its application in integrated circuits. In this paper, a novel generation algorithm of random active shield is proposed using a modified artificial fish-swarm algorithm. By changing the random selection strategy of the generation process, the proposed algorithm makes each selection turn into a successful combination, thus improving the efficiency greatly. Simulations prove that this algorithm is seventeen times faster than the classical Cycle Merging algorithm, while keeping good randomness. Meanwhile, the proposed algorithm is capable of large shield generation. In a 0.18 μm CMOS process with the minimum top-metal width and space of 1.5 μm, the active shield with the area of 3×3 mm^2 only needs approximately 2 h for generation.

1. Introduction

Invasive attacks have already been employed to extracting sensitive information from integrated circuits (ICs) (Anderson and Kuhn, 1996; Handschuh et al., 1999; Quadir et al., 2016; Van Tilborg and Jajodia, 2011). With the help of modern test equipment (Boit et al., 2013; Helfmeier et al., 2013), such as microprobing and focused ion beam (FIB) workstations, invasive attacks can be implemented directly on chips. Attackers can change the connections of internal wires (Ray, 2009), draw artificial pads conducting into the inner circuits and monitor the signals on data buses (Kömmerling and Kuhn, 1999; Weingart, 2000). Therefore, sensitive information like cryptographic keys can be obtained easily. Experiments have proved that these attacks can extract critical information from commercial chips (Tarnovsky, 2008). As a result, the devices and systems, such as computers, embedded devices and intelligent control systems, take integrated circuits as the cores. They have to face the fact that they are unsafe under the threats of invasive attacks.

Various countermeasures (Beit-Grogger and Riegebauer, 2005; Briais et al., 2012a; 2012b; Helfmeier et al., 2012; Manich et al., 2012; Mishra et al., 2017; Ngo et al., 2017; Shi et al., 2016; Xin et al., 2019) are put forward to detect invasive attacks for protecting chips. Some special sensors, such as the capacitance sensor based on ring oscillator (Manich et al., 2012) and the charge sensor with an antenna (Helfmeier et al., 2012), cannot provide protection against microprobing and FIB attacks simultaneously. Particularly, active shield is an effective countermeasure which can resist both of the attacks. Though some backside invasive attacks (Boit et al., 2013; Helfmeier et al., 2013) are given attention because of the circumvention

* Corresponding author at: School of Microelectronics, Tianjin University, Tianjin 300072, China.
E-mail address: yq_zhao@tju.edu.cn (Y. Zhao).
https://doi.org/10.1016/j.cose.2019.06.006
0167-4048/

of the active shield, such attacks are costly and difficult to be performed in some ICs. Reverse engineering must be implemented before the backside attacks to obtain the suitable attack location (Helfmeier et al., 2013). Only after polishing the silicon substrate down to the scale of dozens of micrometers can the subsequent attack steps be performed. All of the extra steps make the implementations of the backside attacks commonly more expensive than those of the frontside attacks. In addition, without the active shield, the frontside attacks will be a better choice rather than the backside attacks because of the easy implementation. Therefore, the active shield is still of great use in thwarting invasive attacks.

Active shield utilizes a complex metal mesh on the topmost metal layer to cover the whole chip. The mesh based on random Hamiltonian path is preferred because of its complex topological structure. However, the random Hamiltonian path is generated in a special way because this path must meet the process requirements. The efficiencies of the available generation algorithms are agonizingly low, which makes them only fit for module-level shield generation. Except an optimization algorithm (Xin et al., 2019), there are few available unoptimized algorithms that mention the capability of large shield generation with the area over 1×10^5 vertices. In this paper, a novel generation algorithm of random Hamiltonian path is proposed using the artificial fish-swarm random-Hamiltonian algorithm (AFSRHA). This algorithm is based on modified artificial fish-swarm algorithm. The AFSRHA has rapid convergence rate and good stability. High execution speed indicates that the AFSRHA is suitable for large shield generation.

The rest of this paper is structured as follows. Section 2 briefly gives the background. Section 3 presents the proposed algorithm in detail. Simulation results are given in Section 4. Conclusions are drawn in Section 5.

2. Background

2.1. Attack methods

Though invasive attacks are sophisticated and expensive requiring advanced technical skills and equipment (Mishra et al., 2017), such attacks are still prevalent and present great threats because they can unearth critical information directly from chips, including the layouts and the stored data in memories, etc. Reverse engineering, microprobing and FIB are three main methods of invasive attacks. Reverse engineering reconstructs the netlist of a circuit by means of layer-by-layer analyses. Attackers are clear about the layout and function of the circuit, so they can do whatever they want to the circuit. Therefore, there are few effective countermeasures to resist reverse engineering at present. Microprobing attack can be utilized to read data on buses or inject faults into internal nets (Mishra et al., 2017). Through the FIB workstation, attackers can cut original tracks and deposit new tracks in a metal layer of a chip (Anderson and Kuhn, 1996). They can also build through-holes to connect nets in the lower layers of the chip. Microprobing and FIB attacks are often combined to form a more effective attack method. Attackers employ the FIB workstation to draw artificial pads connecting with the inner tracks, and then extract information through these pads by microprobing.

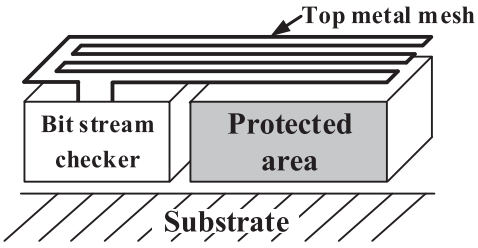

Fig. 1 – Structure of an active shield.

2.2. Detection countermeasures

Several countermeasures against microprobing and FIB attacks have been proposed, which can be divided into two categories. One is the detection of the physical changes during the attack process, such as resistance, capacitance and quantity of electric charge. Salvador Manich presents a design to detect the attack of microprobing (Manich et al., 2012). This detector is based on ring oscillators which monitor the changes of capacitance on data buses. However, this detector needs special time to perform a check, which may influence the data transmission on buses. Clemens Helfmeier proposes a FIB attack detector which checks the variation of charges by a special antenna during the FIB circuit modification (Helfmeier et al., 2012). Nevertheless, this detector can be easily disturbed when the electromagnetic field of environment is strong and unstable.

The other category is barriers. A barrier covers the whole chip and stops access to the inner circuits. Attackers cannot obtain layout information by optical methods. Invasive attacks can be detected by checking if the barrier is modified. Barriers fall into two categories, the passive shield and the active shield. Passive shield utilizes an analogue detector. For instance, the parasitic resistance of a passive shield can serve as a signature. In general, passive shields have simple geometry structures and must tolerate variations in process. There are few studies on passive shield. By contrast, active shield is a research hotspot of the barriers. As is shown in Fig. 1, an active shield is made up of a metal mesh and a bit stream checker. The metal mesh is a mesh of dense metal wires on the top metal layer of a chip (Ngo et al., 2017). The bit stream checker is utilized to check whether the mesh is modified. Compared with passive shields, active shields have more complicated geometry structures. In addition, the detectors of active shields have strong robustness and good tolerance of process deviation. Therefore, active shields are used more wildly.

2.3. Geometry structures

Rerouting attack is the main attack aiming at active shield. Attackers cut off the original metal mesh of an active shield and make new connections through FIB workstation. The new connections result in the invalidation of protection provided by the active shield. The process of rerouting attack is illustrated in Fig. 2.

Please cite this article as: Ruishan Xin, Yidong Yuan and Jiaji He et al., Random active shield generation based on modified artificial fish-swarm algorithm, Computers & Security, https://doi.org/10.1016/j.cose.2019.06.006