TND6321/D
Rev. 0, OCTOBER – 2019

ON Semiconductor®

Anti–tamper Active Shield

© Semiconductor Components Industries, LLC, 2015

October, 2019 – Rev. 0
Publication Order Number:
TND6321/D

ON Semiconductor®

Anti−tamper Active Shield

Abstract

ASIC tampering refers to intentionally changing the functionality of a device or seeking to uncover proprietary secrets in the design or operation of an ASIC. The need for anti−tamper strategies is linked to aerospace and defense applications, but the exponential rise of personal electronics use is driving all market segments to explore anti−tampering methods and offerings.

Introduction

The motives behind a tampering attack will vary. An attacker may be trying to steal services like satellite TV or those available with access cards. Critical data such as company or military secrets, network keys or personal information may be a target, and counterfeiting activities like reverse engineering, stealing or copying intellectual property (IP), and repurposing returned merchandise are common.

There are many aspects to anti−counterfeiting, IP protection, and security, however the first step involved in malicious activities is a basic tampering. Tampering can encompass all forms of obtrusive efforts to gain access to system design, so an anti−tampering strategy and portfolio is becoming paramount, not just for a competitive advantage, but for a basic ASIC offering.

Anti−tamper Active Shield Components

The architecture alone of an active anti−tamper shield satisfies three different components of tampering protection: resistance, detection and evidence. The methodology involving an active shield could also incorporate a tamper response.

An active shield over sensitive areas of a chip combats two specific ASIC tampering attack methods: microprobing and reverse engineering. An attacker will be unable to easily microprobe the IC surface to directly observe, manipulate or interfere with the internal workings of the IC, and any attempt to reverse engineer an ASIC or portions of an ASIC are complicated due to the presence of the active, routed network. The amount of time, tools and talent required to execute a successful attack increase significantly with the implementation of an active shield—and even more so if that active shield is completely random and robust.

A Suggested Strategy

One or more active shields can be incorporated into a design with a transmitter−receiver state machine(s) like the one in Figure 1. The digital circuit itself is simple, but the complexity and security reside in the randomness and robustness of the wire between the transmitter and receiver.

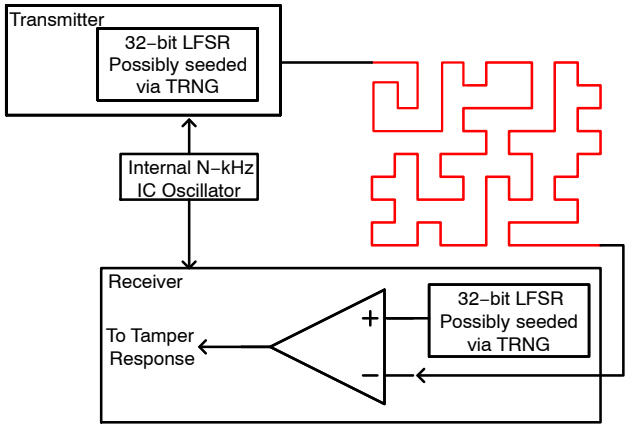

Figure 1.

The transmitter will send a pseudo−random pulse down the wire. The receiver will receive the pseudo−random pulse and compare the sequence. If the shield is cut, then the receiver will not receive the correct sequence, and as such, detect a tamper event. The customer or design engineer can decide if the detection of a tamper will lead to a tamper response such as zeroing out memories, applying a reset or disabling portions of the design.

Table 1.

Name	Type	Dir.	Description
clk	Digital	Input	Clock for the state machine and LFSR counters
xReset	Digital	Input	Asynchronous reset signal used to reset any/all digital logic − asserted low. When *xReset* is asserted, then the *tamper* signal should be deasserted
enable	Digital	Input	Enables the detection circuit. Asserted high. When *enable* is deasserted, then the *tamper* signal should also be deasserted
Seed <31:0>	Digital	Input	Seed value for the LFSR
tamper	Digital	Output	Outputs a logic ‘1’ when a tamper event is detected. Outputs a logic ‘0’ when a tamper event is not detected

Table 1 shows a pinout for an active shield state machine. The seed value can be hardwired to a fixed value, fed from a true random number generator (TRNG) or fed from another source.

When a front end designer incorporates an anti−tamper active shield circuit into a design, the following information would need to be communicated to the layout engineer:

1. How many anti−tamper active shield circuits are included in the design
2. The start and end point(s), i.e. cell instance and pin names
3. What IP, region or regions the shield wire or wires need to cover

The Physical Implementation

ON Semiconductor has developed an algorithm referred to as “Random Orthogonal Plane Filling Curve”, along with a method to generate the random physical architecture of an anti−tamper active shield.

The Physical Design engineer will be responsible for executing the program and incorporating the output anti−tamper active shield wire(s) into the chip layout.

The Algorithm Explained

The “Random Orthogonal Plane Filling Curve” algorithm is described as follows:

1. Start and end coordinate points are chosen. These would most likely be the Q pin of the dataOut flip−flop of the transmitter and D pin of the dataIn flip flop of the receiver for the start and end points, respectively
2. A line is drawn from the start point to the end point
3. The longest segment of the line is identified and a point near the middle is randomly chosen. If multiple segments are of similar length, then a random segment is chosen
4. The chosen segment is then bisected at the chosen point and a line is drawn in a random orthogonal direction until it reaches some sort of blockage. A blockage could be another metal route in the network, the die edge, a bond pad opening, or a defined region boundary
5. Steps 3 and 4 are repeated until the entire plane is filled. Very small holes may appear, but they do not affect the integrity of the shield

This algorithm can be extended to multiple lines where it will first determine which line is the shortest and use it in steps 3 and 4. Doing this, the algorithm will ping−pong between all the lines such that at the end of the fill operation, all lines will be of similar length.

The Algorithm Realized

A developer used a combination of physical design tool capabilities as well as other software to generate a random, top−metal active shield. The physical design engineer can choose to run the program and incorporate the physical geometry of the active shield during the initial floorplanning stage, or they can define a routing blockage over the intended area and bring it into the layout toward the end of the design effort.

The cell instances that encompass the start and endpoint pairs need to be placed and the coordinates of those pairs need to be identified at the onset. A program will ascertain a routing grid and initial beginning lines as illustrated in Figure 2.

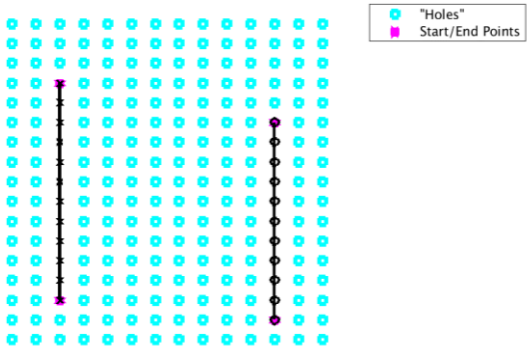

Figure 2.

A first mode will find total length of each line, and choose the shortest line to extend. It will find the lengths of all segments in the chosen network, initially pick longest segment, determine if it is possible create a branch from the center that can be extended out and return. This will be repeated until segments cannot be extended.

A second mode will iterate on the same segment−extending procedure sequentially on each line regardless of total length until segments cannot be extended.

A third mode looks for areas within the grid where routes can be extended to fill in any remaining points on the grid.

When the program completes, it writes out a DEF file containing the geometry for a single, routed wire for each transmit−receive state machine that traverses the entirety of the intended area. When the DEF is read into the physical design tool, the random active shield is visible like something similar to Figure 3. The layout designer can continue with remaining layout tasks and physical design checks.

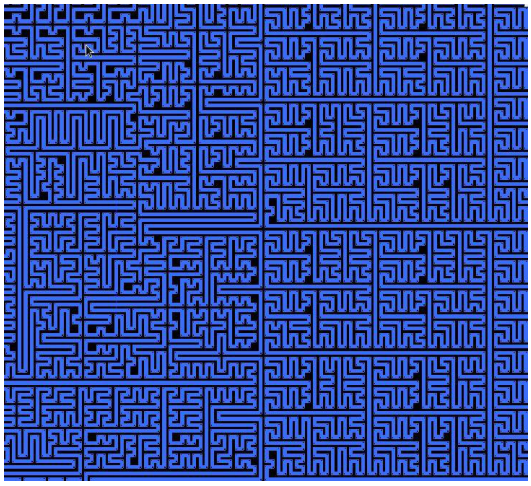

Figure 3.

Conclusion

An anti−tamper active shield is one of the most cost−effective and easy−to−implement anti−tamper tactics. Sheets of metal or floating shapes have been used previously in industry to obstruct circuit visibility and burden reverse engineering efforts. Active shields provide an increased level of security with their tamper resistance, detection, and evidence alone and a tamper response when configured, but they've previously been predictably architected. The complete randomness and the inability to replicate the geometry of the anti−tamper active shield developed with ON Semiconductor's "Random Orthogonal Plane Filling Curve" algorithm provides an even greater level of ASIC security.

ON Semiconductor and ON are trademarks of Semiconductor Components Industries, LLC dba ON Semiconductor or its subsidiaries in the United States and/or other countries. ON Semiconductor owns the rights to a number of patents, trademarks, copyrights, trade secrets, and other intellectual property. A listing of ON Semiconductor's product/patent coverage may be accessed at www.onsemi.com/site/pdf/Patent−Marking.pdf. ON Semiconductor reserves the right to make changes without further notice to any products herein. ON Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does ON Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation special, consequential or incidental damages. Buyer is responsible for its products and applications using ON Semiconductor products, including compliance with all laws, regulations and safety requirements or standards, regardless of any support or applications information provided by ON Semiconductor. "Typical" parameters which may be provided in ON Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals" must be validated for each customer application by customer's technical experts. ON Semiconductor does not convey any license under its patent rights nor the rights of others. ON Semiconductor products are not designed, intended, or authorized for use as a critical component in life support systems or any FDA Class 3 medical devices or medical devices with a same or similar classification in a foreign jurisdiction or any devices intended for implantation in the human body. Should Buyer purchase or use ON Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold ON Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that ON Semiconductor was negligent regarding the design or manufacture of the part. ON Semiconductor is an Equal Opportunity/Affirmative Action Employer. This literature is subject to all applicable copyright laws and is not for resale in any manner.

PUBLICATION ORDERING INFORMATION

LITERATURE FULFILLMENT:
Literature Distribution Center for ON Semiconductor
19521 E. 32nd Pkwy, Aurora, Colorado 80011 USA
Phone: 303−675−2175 or 800−344−3860 Toll Free USA/Canada
Fax: 303−675−2176 or 800−344−3867 Toll Free USA/Canada
Email: orderlit@onsemi.com

N. American Technical Support: 800−282−9855 Toll Free USA/Canada
Europe, Middle East and Africa Technical Support:
Phone: 421 33 790 2910

ON Semiconductor Website: **www.onsemi.com**

Order Literature: http://www.onsemi.com/orderlit

For additional information, please contact your local Sales Representative