SECURE-IC
THE SECURITY SCIENCE COMPANY

PRODUCT SHEET

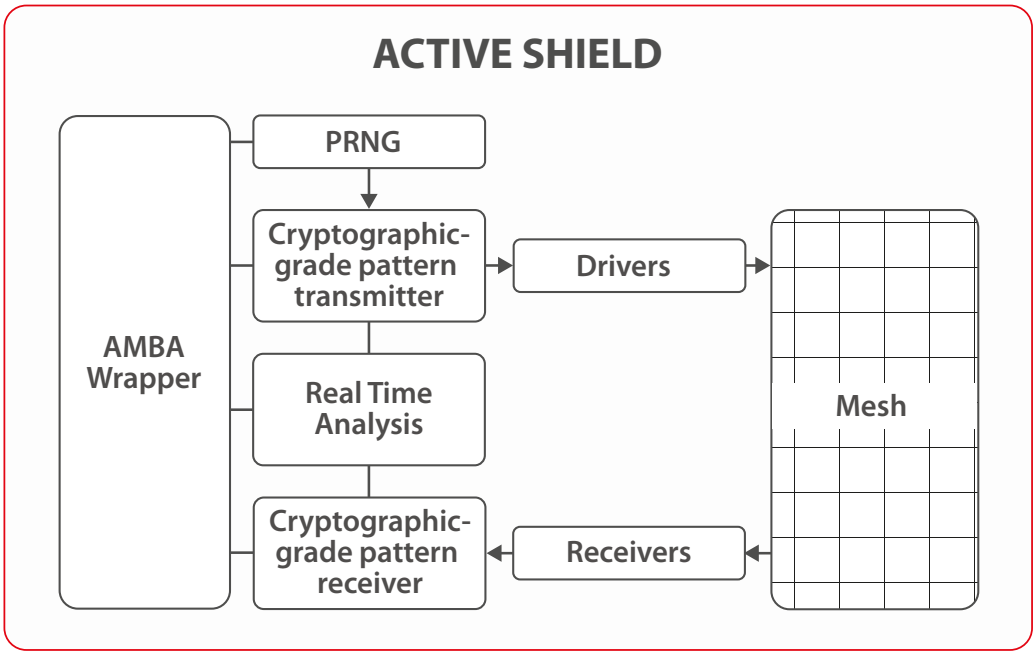
Securyzr™ > Securyzr™ Secure HW Solutions >Securyzr™ Security IP > Anti-Tamper > Active Shield > SCZ_IP_AS_200

ACTIVE SHIELD

Attacks on digital circuits can occur when an attacker attempts to physically alter the device's internal components. These types of attacks are known as intrusive and can include actions such as probing or manipulating signals, adding or removing components, or modifying features on the chip.

To counteract these threats, Secure-IC has developed the Active Shield technology. This technology uses a protective mesh layer over the sensitive parts of the circuit, and actively monitors the mesh integrity for any signs of tampering. This countermeasure helps to safeguard the circuit's features and components, such as metal routing and transistors, from unauthorized access or modification through the front side of the device, such as:

- Wire micro-probing to read or force an equipotential
- Wire cutting (e.g., alarms, entropy source disconnection from a true random number generator…)
- Wire re-routing
- Burnt fuses opening
- ROM Altering



Features

- Anti-tamper solution with a mesh placed over the sensitive parts of the circuit and actively monitored
- Uses random cryptographically generated patterns to detect integrity violations
- Antenna-effect safe
- Security certification ready (incl. Common Criteria)
- Fully digital and designed with the standard cells library
- Mesh designed with scripts
- Mesh can be interleaved with P/G network in topmost layers (no need to sacrifice a layer)
- Compatible with clock gating to reduce the power consumption
- Transferable to any design kit
- Lightweight
- No calibration after design
- Easy to integrate into the system
- AMBA (APB, AHB, AXI) interface

Applications

- IoT
- Setup Box
- Mobile
- Automotive
- Defense

Active monitoring

In order to further deter intrusive attacks, the mesh is actively monitored using random cryptographically generated patterns to detect integrity violations. By using this technology, modifying and rerouting the mesh becomes very costly as the attacker must reroute many wires to avoid detection. In addition, the data travelling through the shield mesh cannot be predicted by the attacker, because it is output by a cryptographic block cipher.

Active Shield technology relies on several submodules:

- A mesh created using a metal layer for wire routing
- Drivers and receivers used for electrical connection with the mesh
- A cryptographic-grade tamper detection module for monitoring the mesh integrity

Ideal for

Active Shield IP is ideal for:

- Protection against Bus probing
- Protection against FIB attacks
- Protection against wire micro-probing to read or force an equipotential
- Protection against wire cutting (e.g., alarms, entropy source disconnection from a true random number generator)
- Protection against wire re-routing
- Protection against ROM altering

Deliverables

- Technical specifications
- RTL of the AMBA wrapper
- Constraints file (SDC)
- Remote support for integration
- User guide
- Post-synthesis generic netlist
- Innovus Back-end scripts (TCL) to place and route the mesh
- Test report documentation
- Self-checking RTL Testbench based on reference scenario for simulation. (Simulation scripts are adapted to Questasim, any change of Simulator shall be taken care of by the Licensee)

V1.2

SECURE-IC
THE SECURITY SCIENCE COMPANY

HEADQUARTERS
Digital Park B - ZAC Atalante Via Silva
801 avenue des Champs Blancs
35510 Cesson-Sévigné - France
+33 (0)2 99 12 18 72 - contact@secure-ic.com

EMEA
sales-EMEA@secure-ic.com

AMERICAS
sales-US@secure-ic.com

APAC
sales-APAC@secure-ic.com

JAPAN
sales-JAPAN@secure-ic.com

CHINA
sales-CHINA@secure-ic.com

CONTACT US

www.secure-ic.com