Definition of Hardware Trojan (HT)

A Hardware Trojan is a malicious, undesired and intentional modification of an integrated circuit or design. It can transmit critical information without the knowledge of the user or disable/destroy some components of the circuit.

A HT insertion can be done at any stage during the design of an integrated circuit or during the manufacturing process.

Detection of Hardware Trojan

Detection

Destructive

Built-in-test

Non-destructive

Logical tests

Side Channel

Detection of a HT can use several techniques. The side channel approach is one of the most studied methods through the power/temperature/electromagnetic emissions analysis.

Measurements of data path delay

A set-up time violation may arise if the last signal transition is too close to the clock’s rising edge. The violation of the timing constraint permits to inject faults into a integrated circuit.

The clock glitch (fig 1) is achieved by progressively reducing the clock period, until a setup time violation occurs.

The choice of the injection’s cycle is possible.

Generate a fault leads us to measure the bits propagation time knowing the number of $\Delta T$ diminution (fig 2).

RTL modifications

The measured path delays’ distributions of an AES without HT, and one with a HT (fig 4) were done on the same board. The mean path delay associated to each bit has significantly changed. Their “orders of appearances” and the distribution of the “ghost bits” have been changed. The modifications (fig 5) induced by the HT are significant.

Conclusion

The distribution of those propagation times is a characteristic “fingerprint” of the module, suggesting that this might be a practical means of authenticating an IP and also a method to qualify the integrity of a given IP, without adding any other circuit.

Exurville Ingrid*,$^\dagger$, Fournier Jacques*,$^\ddagger$, Dutertre Jean Max*,$^\dagger$, Robisson Bruno*, Tria Assia*$^\ddagger$

*CEA, $^\ddagger$EMSE

880, route de Mimet, 13541 Gardanne, France