IC Trojan horse is a serious technical problem faced by SOC developers. Most of the SOC developers use third party IP components for their design purpose. So comparing with a Trojan-less counterpart is impossible. Villasenor and Kim proposed bus architecture to detect Trojan activity where, when the circuit realizes the presence of a Trojan, it informs the CPU by an interrupt. In this paper, we are improving the bus architecture by proposing one more potential Trojan horse existence condition and also give a method to identify the exact cause that initiated the Trojan initiation. Then, we try to propose improvements to the bus architecture to make the thwarting and detection faster and efficient by using the obtained results of the above circuits.

References

- Villasenor. J. D and Lok-Won-Kim,"A system-on-chip bus architecture for thwarting integrated circuit trojan horses, IEEE transactions on very large scale integration (VLSI) circuits. pages-1921-1926
2008, pp. 87 – 95.
  - AMBA specification
  - Susmit Jha and Sumit Kumar Jha, "Randomisation based probabilistic approach to
  - Jim Plusquellic, University of New Mexico, "Taxonomy of Trojans for IC Trust.
  - Y. Jin and Y. Makris, "Hardware Trojan detection using path delay
fingerprint," in IEEE International Workshop on Hardware-Oriented Security and Trust
(HOST&apos;08), 2008, pp. 51 – 57.
  - R. Rad, J. Plusquellic, and M. Tehranipoor, "Sensitivity analysis to hardware
Trojans using power supply transient signals," in IEEE International Workshop on
Hardware-Oriented Security and Trust (HOST&apos;08), 2008, pp. 3 – 7.
  - M. Banga and M. S. Hsiao, "A novel sustained vector technique for the detection
332.
  - M. Abramovici and P. L. Levin, "Protecting integrated circuits from silicon Trojan
and implementing malicious hardware," in Proceedings of the 1st Usenix Workshop on
Large-Scale Exploits and Emergent Threats (LEET). San Francisco, California: USENIX
  - T. Kean, D. McLaren, and C. Marsh, "Verifying the authenticity of chip designs
with the Design Tag system," in IEEE International Workshop on Hardware-Oriented
Security and Trust (HOST&apos;08), 2008, pp. 59 – 64.
  - R. S. Chakraborty, S. Paul, and S. Bhunia, "On-demand transparency for
improving hardware Trojan detectability," in IEEE International Workshop on
Hardware-Oriented Security and Trust (HOST&apos;08), 2008, pp. 48 – 50.
no. 4, pp. 20 – 27, 1997.
  - A. Goel and W. R. Lee, "Formal verification of an IBM CoreConnect processor
  - F. Lin, H. Wang, and J. Bian, "Hw/sw interface synthesis based on Avalon bus
  - X. Xing, C. Zezong, J. Jing, and K. Hengyu, "Porting from
wishbone bus to avalon bus in soc design," in Electronic Measurement and
  - S. Murali and G. D. Micheli, "An application-specific design methodology for
Proceedings, 2005, pp. 1176 – 1181
  - D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan
detection using IC fingerprinting," in IEEE Symposium on Security and Privacy
(SP&apos;07), 2007, pp. 296 – 310.
  - F. Wolff, C. Papachristou, S. Bhunia, and R. Chakraborty, "Towards Trojan-free
trusted ICs: problem analysis and detection scheme," in Proceedings, Design Automation
and Test in Europe (DATE&apos;09), Munich, Germany, March 10-14, 2008, pp. 1362 – 1365.

**Index Terms**

Computer Science  
Security

**Keywords**

Soc  Amba trojan Circuit xilinx  spartan