Authenticate ICs using Blockchain

Altahan Mohammad

Master thesis in Computer Science

In this work, we provide a way to prevent Counterfeiting crimes on ICs (Integrated circuits). We present a mechanism to authenticate ICs on their way from the manufacturer to the customer using Physical Unclonable Function (PUF) based ICs and blockchain technology. The combination of PUF based ICs and blockchain is programmed as a defence mechanism against counterfeiting attacks. These attacks aim to steal the design and extract knowledge from within the ICs. Once the attackers obtain the information, they can produce clones and perform malicious attacks.

Our project uses state-of-the-art technologies to authenticate and monitor ICs. The authentication process is done by PUF based IC and the monitoring of the status of the ICs by blockchain. We provide a micro python implementation for the authentication part on the PUF based IC side i.e. message signing, digital signature generation, and socket server. In order to achieve confidential communication between the client, the socket server and between the clients themselves, we implement an interface based on blockchain technology. By using this combination, we increase the level of security to protect ICs and secure them against counterfeiting activities.

Prof. Jacques Pasquier