Research statement

We wish to submit a new proposal entitled **"**Detecting and Preventing counterfeit Hardware by Scalable and Reliable Logic Locking" to be considered by IPM.

Due to the increasing cost of maintaining integrated circuits foundries with technology scaling, many chip designers have become fabless and created a globally distributed integrated circuits supply chain wherein integrated circuits fabrication, testing, and packaging are outsourced to off-shore foundries. To protect designs against a number of important attacks, such as cloning, overproduction, or unauthorized integration, we propose a performance-aware scalable and reliable logic locking method (SRLL) that can be applied to high-performance designs. In this research, we aim to show a scalable and reliable hardware encryption framework based on two concepts: logic locking and obfuscation. SRLL is a design-for-security solution that modifies the design in such a way that the correct output cannot be produced unless the design is activated with the correct key. Therefore, only the authenticated user will be able to correctly activate the design. In our proposed approach, the designer adds post-manufacturing programmability into the design controlled by programmable values referred to as the key. Our aim is to find a new trade-off point that provides the same security guarantees of traditional logic locking while achieving high performance. To enable this, we limit the logic locking functions to non-critical path components of the circuit. Using this method, we show early work that provides higher performance than previous works. We evaluate SRLL on ISCAS′85 and MCNC′91 benchmarks to provide security and performance analysis of our proposed method. Our current work shows promise as we can see exponential resiliency against SAT-based attacks while maintaining a reasonably low-performance overhead.

Siamak Mohammadi, Ph.D
Associate Professor in School of Electrical and Computer Engineering
University of Tehran