Research Directions for Crypto-Physically Secure TEEs

Sylvain Bellemare*

September 14, 2024

Information is not a disembodied abstract entity; it is always tied to a physical representation. It is represented by engraving on a stone tablet, a spin, a charge, a hole in a punched card, a mark on paper, or some other equivalent.

Rolf Landauer
The physical nature of information

Abstract

This is an initiative to spark research to explore how we could develop a secure chip for TEEs (Trusted Execution Environments) that would ultimately be secure because of physics rather than economics. Current commercial TEEs do not offer protection against side-channel and physical attacks. Making the cost of a physical attack expensive is the only current known defense mechanism. Thus, TEEs are ultimately only secure through economics. The chip design should be open source, and its physical implementation should be verifiable, meaning that it should match the open source design. Moreover, the root of trust (embedded secret key) should be proven to have not leaked during generation or manufacturing and be tamper resistant for the lifetime of the device that it secures. Thus, the hope and vision is to develop a TEE chip that can be trusted because it can be verified by physics and mathematics.

*Cornell Tech, New York, sbellemare@cornell.edu.