# IST 597 Project Report Wrapper

Yufei Jiang

## 1 The Difference between Intel SGX and ARM TrustZone

### 1.1 Overview

Trusted Computing (TC) is a concept developed by the Trusted Computing Group. It has been discussed for years. Regarding the meaning of "trusted", there are a lot of controversy. Some people also challenge the idea of Trusted Computing fundamentally since it may be harmful to keep anonymity over Internet and avoid vendor-lock-in. Despite the buzz, some players in the technical industry, including Dell, HP, Microsoft, Intel, and ARM have made solid progress on realizing this concept.

In this report, we will investigate two concrete Trusted Computing solutions. They are Intel SGX and ARM TrustZone. According to the definitions given by Trusted Computing Group. A complete Trusted system must have the following 6 elements: endorsement key, secure input and output, memory curtaining, sealed storage, remote attestation, and trusted third party. More specifically, both Intel SGX and ARM TrustZone are two measurements to fulfill memory curtaining part in the whole Trusted system.

In the following subsections, we will first briefly introduce Intel SGX and ARM TrustZone respectively. Then we will compare them two from certain aspects.

### 1.2 Intel SGX

The full name of Intel SGX is Intel Software Guard Extensions. Intel SGX is a technology to help developers better protect the confidentiality and integrity of selected code and data of their applications from those rogue software that is running in higher level including the operating system. It was implemented in 6th generation Intel Core microprocessors in 2015 for the first time. Its basic mechanism is to create some protected areas in memory which are called "enclaves". Developers can explicitly use Intel SGX SDK during the development to put the data and code of interests into enclaves.

## 1.3 ARM TrustZone

## 1.4 Comparison

### 1.4.1 Architecture

### 1.4.2 Development

Right now Intel SGX only provides enclave binding API in C and C++.

### 1.4.3 Invocation

### 1.4.4 Encryption

### 1.4.5 Security

### 1.4.6 Lifecycle

### 1.4.7 Adoption

Intel SGX is different from ARM TrustZone. Architecturally, with ARM TrustZone, a CPU is in two halves which are insecure world and the secure world. Any communication occurs from the insecure world to the secure world is via the Secure Monitor Call (SMC) instruction. At the meanwhile, in Intel SGX model, there is only one CPU with many secure enclaves. Conceptually, Intel SGX is similar to "Protected Process" which is implemented in Microsoft Windows Vista for the first time. However, Intel SGX is safer since it is enforced by hardware.

Regarding ARM TrustZone, ARM is historically associated with so called "single- purpose systems". The System on Chip (SoC) is customized to some specific markets (e.g. smartphones) so there is only one "Trust Zone". Intel SGX has multiple enclaves in a system. So it can be used in a more general multi-purpose chips.

Test [1]

# References

[1] "Church encoding," http://goo.gl/I03nLI, accessed: 2015-04-22.