

# Intel SGX e Criptografia Homomórfica

Gabriel G. Milan<sup>1</sup>, Natã Carvalho<sup>1</sup>, Brenno Rodrigues<sup>1</sup>

<sup>1</sup>Departamento de Engenharia Eletrônica e de Computação – Universidade Federal do Rio de Janeiro (UFRJ)  
21.941-909 – Rio de Janeiro – RJ – Brasil

**Abstract.** *This document is the report of a work of the discipline of "Information Security"(NCG020) at the Federal University of Rio de Janeiro (UFRJ). The work consists of conducting research on the Intel SGX platform and homomorphic cryptography, in order to obtain brief knowledge of these subjects.*

**Resumo.** *Esse documento é o relatório de um trabalho da disciplina de "Segurança da Informação" (NCG020) na Universidade Federal do Rio de Janeiro (UFRJ). O trabalho consiste em realizar uma pesquisa sobre a plataforma Intel SGX e criptografia homomórfica, a fim de obter breve conhecimento nesses assuntos.*

## 1. Introdução à Intel SGX

A Intel SGX consiste em particionar informações confidenciais em “enclaves”, como denominado pela própria Intel, que são áreas de execução na memória com maior proteção.

A plataforma, que nasceu devido à dificuldade dos desenvolvedores de garantir segurança em suas aplicações, promete:

- Aumentar integridade e confidencialidade;
- Atestar e provisionar remotamente;
- Ajudar a reduzir significativamente maneiras de ataque;
- Baixa curva de aprendizado.

Denominando-se uma nova abordagem, embasa-se em incrementos na arquitetura do hardware, com instruções específicas para segurança de aplicações.

Como pode ser visto na Figura 1, em tempo de execução, as instruções constroem e executam os enclaves em uma região especial e cifrada da memória com acesso restrito definida pelo desenvolvedor. Isso ajuda a prevenir vazamento de dados, uma vez que tudo que está contido nos enclaves é cifrado e possui sua integridade verificada.

Na Figura 1, os números significam:

1. Aplicação construída com partes seguras (SGX) e partes não-seguras;
2. Quando o aplicativo roda, cria a enclave, que é colocada na área segura de memória;
3. Quando uma função segura é chamada, a execução transita para a enclave;
4. A enclave consegue visualizar todos os dados de maneira plana, ainda que impedindo acesso externo não autorizado;
5. A função retorna, mantendo os dados sensíveis na região protegida da memória;
6. A aplicação continua seu curso normal.

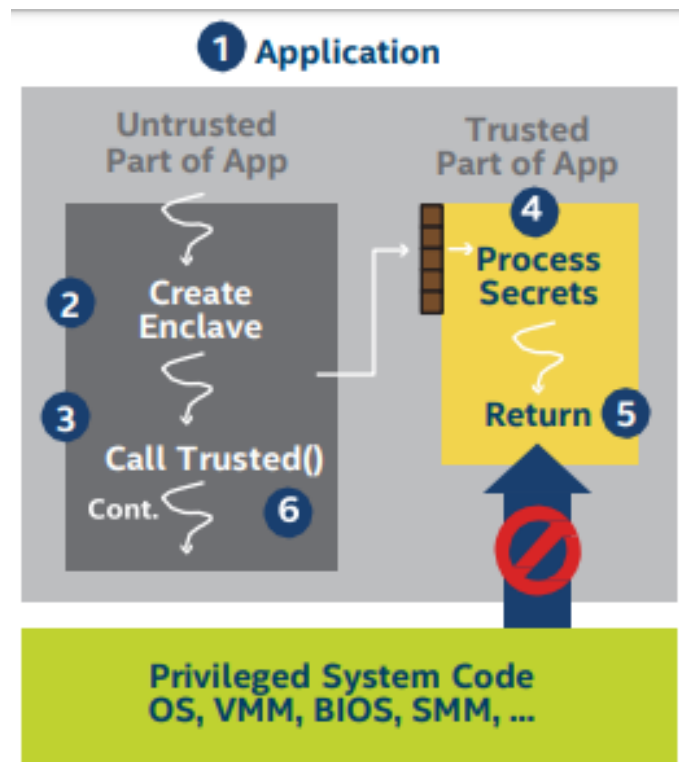


Figura 1. Execução

## 2. Casos de uso da Intel SGX

A Intel cita alguns casos de uso interessantes para sua plataforma, vistos a seguir:

### 2.1. Gerenciamento de chaves

Usar enclaves para ajudar a gerenciar chaves criptográficas e fornecer funcionalidades semelhantes a de um HSM.

### 2.2. Blockchain

Ajuda a aumentar a privacidade e segurança para o processamento de transações, consenso, contratos inteligentes e armazenamento de chaves.

### 2.3. Aplicações em tempo de execução

Permite executar aplicações sem nenhuma alteração dentro de enclaves.

### 2.4. Proteção de conteúdo aprimorada por hardware

Ajuda proprietário de conteúdo a proteger seus IPs por meio de streaming inalterado ou não modificado.

### 2.5. Carteiras digitais

Pode ser usada para garantir mais segurança em transações monetárias.

### 2.6. IoT

Pode permitir uma conexão mais segura com dispositivos IoT.