TEE と REE のメモリアクセス性能に関する一考察

柴田俊哉 [1]　山口実靖 [1]

1. はじめに

クラウドコンピューティングが普及し，多くの状況で活用されるようになっている．一方で，自身の機密データを自身が管理しない計算機上にアップロードすることに対する不安や懸念も指摘されている．特に，クラウドシステムの OS(Operating System オペレーティングシステム)を提供するクラウド事業者が悪意のある OS を用意しそれをユーザに使用させた場合は，ユーザとしてこれの不正に対応することの難しさが指摘されてきた．

この課題に対して，CPU に TEE(Trusted Execution Environment)を機能を持たせ，OS からも攻撃することができない TEE にて機密性の高い処理を実行する手法が提案されている．一方で，TEE 内でプログラムを実行すると性能が低下することも指摘されている．本ポスター発表では，TEE におけるメモリアクセス性能を評価し，TEE 内で動作するプログラムの性能向上手法について考察を行う．

2. 関連研究

2.1 TEE

TEE[1]は CPU が持つ機能であり，メモリの一部に OS からも攻撃することができない暗号化領域を作成し，その中でプログラムを動作させる．CPU はその外部にあるメモリを管理することができないが，信頼領域なのデータは暗号化してメモリに保存するため，悪意のある OS やハードウェア(マザーボードやメモリ)であっても，復号したデータを取得することができない．一方で，データが暗号されるなどのオーバーヘッドが伴うため，TEE 内における処理の性能は，REE(Rich Execution Environment, 信頼領域でない通常の領域)[2]との指摘もされている．

2.2 TEE の性能

Suzaki らは TEE と REE における演算やメモリアクセスの性能を比較し，TEE における処理の性能が REE より低いことなどを示している[2].

3. 性能評価

一定量のメモリを確保し，そのメモリのすべてに読み込みアクセスを行うことを 1000 回繰り返すマイクロベンチマークを作成し，それに TEE および REE で実行したときに要する時間を評価した．計測は Intel SGX を用いて行った．

データサイズと所要時間の関係を図 1 から図 2 に示す．両図より，アクセスデータサイズが約 96MiB を超えるとメモリアクセス性能が大幅に劣化することが分かる．これは，SGX の EPC(Enclave Page Cache)内のユーザが使用可能な領域のサイズが 96MiB であるためである．

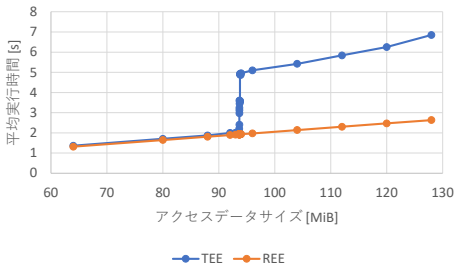

図 1 アクセスデータサイズとアクセス時間

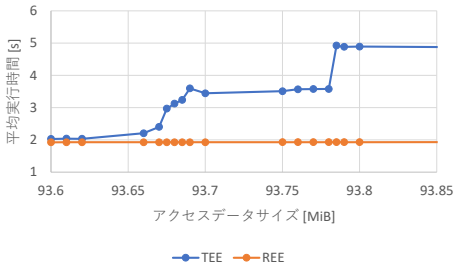

図 2 アクセスデータサイズとアクセス時間 (拡大)

また，データサイズが 1MiB から 32MiB の 1 バイトあたりの読み込み時間と CPU キャッシュの参照回数/ミス回数を図 4，図 5 に示す．

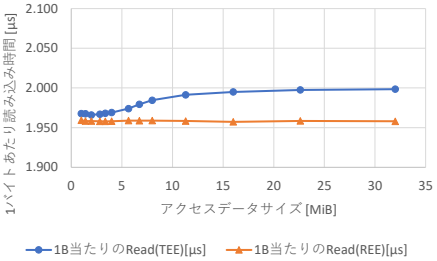

図 3 アクセスデータサイズと 1 バイトあたりのアクセス時間

1 工学院大学
Kogakuin University

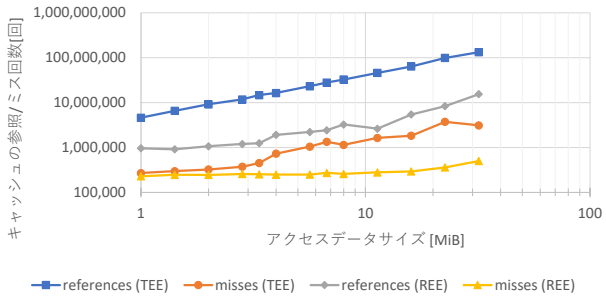

図 4 アクセスデータサイズとキャッシュの参照回数/ミス回数

TEE と REE におけるメモリアクセスの性能には大きな差が確認できないが，キャッシュ参照回数やキャッシュミス回数においては大きな差があることが確認された．

4. おわりに

本ポスター発表では，TEE と REE におけるメモリアクセス性能を評価した．

謝辞 本研究は JSPS 科研費 21K11854, 21K11874 の助成を受けたものである．

参考文献

[1] M. Sabt, M. Achemlal and A. Bouabdallah, "Trusted Execution Environment: What It is, and What It is Not," *2015 IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, 2015, pp. 57-64, doi: 10.1109/Trustcom.2015.357.

[2]K. Suzaki, K. Nakajima, T. Oi and A. Tsukamoto, "TS-Perf: General Performance Measurement of Trusted Execution Environment and Rich Execution Environment on Intel SGX, Arm TrustZone, and RISC-V Keystone," in IEEE Access, vol. 9, pp. 133520-133530, 2021, doi: 10.1109/ACCESS.2021.3112202.