開発テーマ名

Super Creator

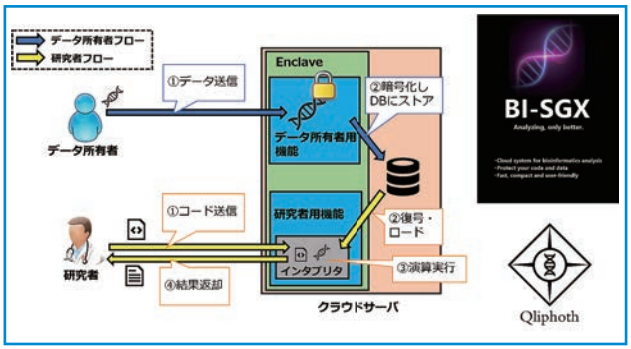
生命情報解析向けインタプリタを搭載した秘密計算用クラウド

櫻井　碧
さくらい　あお

《略歴》
1995年　埼玉県生まれ
2014年　早稲田大学 基幹 理工学部 学系II (情報理工学科) 入学
2018年　早稲田大学 基幹理工学部 情報理工学科 卒業
2018年　早稲田大学 大学院 基幹理工学研究科 情報理工・情報通信専攻 入学
2020年　早稲田大学 大学院 基幹理工学研究科 情報理工・情報通信専攻 卒業
2020年　日本IBM 株式会社 入社
《受賞歴》
2018年10月　早稲田大学 Computer Science Student Workshop　優秀賞
2019年10月　早稲田大学 Computer Science Student Workshop　最優秀賞
2020年 3月　一般社団法人 情報処理学会SIGBIO優秀プレゼンテーション賞 (BIO研究会) (2019年度)
《所属》※ 2020年5月現在
日本IBM 株式会社 GBS部門 ITスペシャリスト

テーマ概要

遺伝子情報をはじめとした生命情報は、極めてセンシティブな情報であるため、データ漏洩には特別の注意を払わねばならない。このような機密情報の中身を見ないままに、匿名化された統計情報のみを結果として取得する技術として、秘密計算という技術が存在する。数ある秘密計算技術の中でも、Intel SGXと呼ばれるCPUによるRAM上のデータを保護する機能が、秘密計算の要件を実用的に実現する上で注目されている。しかし、SGXを用いたプログラムの開発には極めて煩雑で難解な「SGXSDK」というSDKを使用しなければならない。これは開発者に莫大な負担をかけるため、SGXが敬遠される最大の要因になっている。そこで、本プロジェクトではSGXがRAM上に形成する保護領域上でインタプリタを駆動させ、独自の明快な言語「Qliphoth」を提供することで、高い安全性とパフォーマンスを提供しながらも利用難易度を低く抑えた、生命情報解析向けクラウドシステム「BI-SGX」を開発した。「BI-SGX」は、GWASのような生命情報解析は勿論、より汎用的な処理についての秘密計算も可能とする、実用的な秘密計算向けクラウドとなっている。



藤井 PM の評価

Intel SGXを活用し、生命情報解析向けの秘密計算クラウドプラットフォーム「BI-SGX」をプロジェクト期間中に開発した。単にIntel SGX活用の可能性を証明しただけではなく、実利用を想定したEnclaveへのデータ転送、インタプリタ、ゲノムワイド関連解析（GWAS）なども実装されており、まさに生命情報解析向けの秘密計算プラットフォームと言える。Intel SGX環境という、非常に制約の多く、また厳しいプログラム開発環境において本プロジェクトを完遂したことは、プログラマとしても高く評価されるべきである。Microsoft AzureなどのクラウドでもIntel SGXを活用できるベアメタルサーバが活用できる時代になっている。BI-SGXが国内だけにとどまらず、グローバルに活用されることを期待している。

近況メッセージ

・開発成果の近況、展開方針、今後の目的など

現時点では、「BI-SGX」の高速化に主眼を置いて改良を試みている。例えば、保護領域の境界を跨ぐ関数呼び出しを高速化するSGXの機能の採用や、インタプリタ本体のアルゴリズムの改良といった内容である。また、Qliphothライブラリを開発者が簡単に実装することを可能とし、かつそれを内部で自動的にSGXのAPIを用いて記述されたBI-SGXの言語処理系コードに変換するツールの設計・開発に向けた準備も進めている。

今後は、完全無料で利用できる「BI-SGX」をより世間に認知してもらえるように、宣伝を活発化させたいと考えている。

・近況

就職により時間的制約は大きくなっているが、「SGXSDK」の難解さに苦しむ開発者の相談を受け、適切な実装方法等解決策を提示するような無料のボランティアを行っている。また、SGXを絡めたマルチスレッド処理を希望する開発者向けに、簡単にSGX上での並列処理を利用出来るような汎用的なフレームワークの開発にも勤しんでいる。同時に、SGXのようなTEEを用いたHIEE技術についての知識をより汎用的なものにする為に、AMDやRISC-V等がそれぞれ提供するTEE技術についてのサーベイも進めている。

関連 URL

https://github.com/hello31337/BI-SGX
https://bi-sgx.net