開発テーマ名

Super Creator

準同型暗号によるバーチャルセキュアプラットフォームの開発

松本　直樹
まつもと　なおき

《略歴》

2017年3月　愛媛県立松山東高等学校 卒業

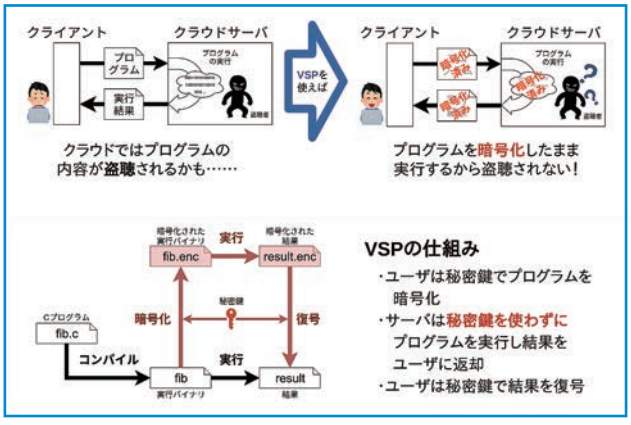
2017年4月　京都大学 工学部 情報学科 入学

《所属》 ※ 2020年5月現在

京都大学 工学部 情報学科 4年

テーマ概要

本プロジェクトでは準同型暗号を用いてデータ・プログラム両方を暗号化したまま計算処理を行うことで、クラウドコンピューティングのような攻撃者のハードウェアへのアクセスが制限できない状況でも安全なオフローディングを実現する、バーチャルセキュアプラットフォームを提案、実装した。根幹となるアイデアは、プロセッサの論理回路を準同型暗号上の演算に置き換えることである。我々の実装は暗号上の1クロックサイクルを最短で約1.5sで評価することができる。我々は本プロジェクト実現にあたり、準同型暗号ライブラリ、準同型暗号の並列実行エンジン、ISAとCPU、LLVMバックエンドなどを開発した。全ての成果はオープンソースで公開されている。



首藤 PM の評価

準同型暗号に基づく、高級プログラミング言語を用いた任意処理の秘密計算、それを世界で初めて実装・実現した。得意分野が異なる、並外れた腕を持つクリエータ3人が奇跡的にぴったりと噛み合い、これほどの成果物に結実した。松本君は、主に、プロセッサの設計・開発を行った。プロセッサの命令セットアーキテクチャ（ISA）設計は3人で行った。

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

成果報告会後は、VSP全体の性能向上を目指してプロセッサ設計の改良を行い、スーパースカラのプロセッサ設計をVSPに組み込みました。また、実験的実装であったマルチGPU対応のライブラリも正式に組み込みました。3月には研究者の方たちとの意見交換会を行い、現在は論文の執筆でプロセッサの設計に関する部分を担当しています。今後は、VSPの高速化だけでなくVSPや他の関連技術を組み合わせた応用ソフトウェアのアイデアが既にあるので、それらの開発を進めていきたいと考えています。

・近況

4月から研究室に配属され、ネットワークや分散処理について勉強・研究を進めています。アルバイトではRFCを読みながらサーバーのフルスクラッチや実験実装を行い、技術を磨く日々を過ごしています。未踏期間中はひたすらアウトプットの連続であったため、今は新しい言語に触れたり、OSS のプラグインを書くなど、今まで関わったことがなかった分野に触れ、インプットを積極的に行っています。今までは作って終わりにすることが多かったのですが、今後は作ったものを育てていくということをしていきたいと考えています。

関連 URL

https://github.com/virtualsecureplatform