開発テーマ名

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

Super Creator

松岡　航太郎

まつおか　こうたろう

《略歴》

2017 年 3 月　東京都立戸山高等学校 卒業

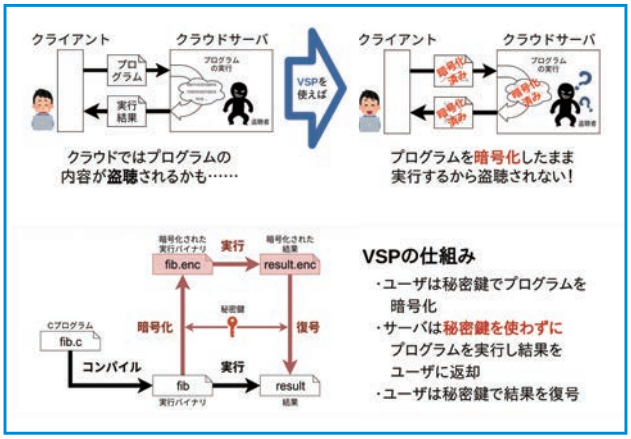
2017 年 4 月　京都大学 工学部 電気電子工学科 入学（特色入試）

《所属》 ※ 2020 年 5 月現在

京都大学 工学部 電気電子工学科

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。松岡君は、プロジェクトの発案、チームの編成、準同型暗号ライブラリの開発等を行った。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

現時点でUSENIX　SECURITY　2021に出すべく論文を執筆中。また、論文を書くにあたっての評価のために成果を拡張している。論文執筆後は思いついてはいるが適用できていない最適化が幾つか存在するため、それらを適用していきたい。

本テーマはPoCと位置づけているが、「トラストレスな計算処理のオフローディング」が根幹的なアイデアであるので、Garbled Circuitなどの他の技術も取り入れることも含めてセキュリティや実行性能などの点でよりよい形を考え、実用に近づけていくつもりだ。

・近況

4回生の特別研究として最近は計算電磁気学をやっている。暗号とはまた違った数学で興味深い。本テーマの過程で書いたCUDAも高校来の夢だったが、シミュレーションもそのひとつなので技能を身に着けたいと思っている。現時点で大学院では、未踏と同じ秘密計算をやるつもりだ。

今は論文を書くので手一杯でなかなか他のことができていないが、家にずっと居るので分割キーボードを作ろうと思っている。やってみて準同型暗号は専門家が少ないということを感じたので、今後も独学ではあろうが準同型暗号について知識を深めたいと考えている。

関連 URL

https://github.com/virtualsecureplatform/kvsp