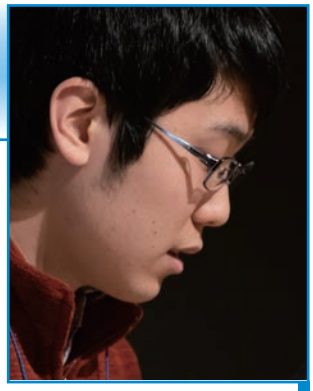
開発テーマ名

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

伴野　良太郎

ばんの　りょうたろう



《略歴》

1998年10月　大阪府生まれ

2002年　奈良県に引っ越す

2017年 3月　東大寺学園高等学校 卒業

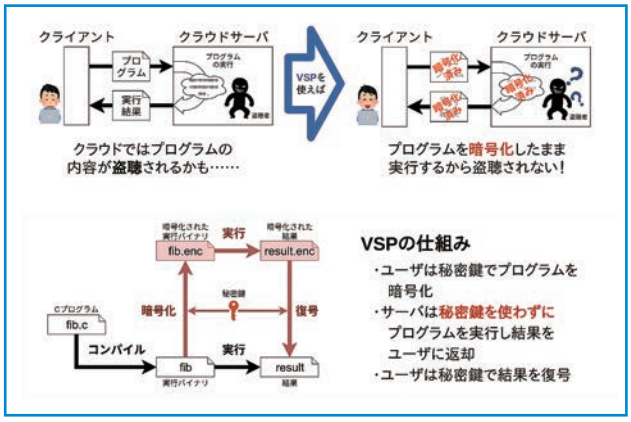
2017年 4月　京都大学 工学部 情報学科 入学

《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。伴野君は、主に、C言語コンパイラの開発を行った。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

現在はVSPに関する論文執筆を行っていて、私は主にコンパイラや「Iyokan」（ゲート評価エンジン）に関する部分を担当しています。同時に「KVSP」の開発も継続しています。4/13にリリースした「KVSP v11」ではコマンドライン引数をプログラムに与えられるようになり、また5/4にリリースした「KVSP v15」では必要に応じてROMやRAMの構成方法を変えられるようになりました。今後は「KVSP」のさらなる高速化や、「KVSP」を基盤に用いたアプリケーションに目を向けられたらと考えています。

・近況

新型コロナウイルスの影響で大幅に遅れながらも、無事B4として研究室に配属されました。今後はプログラム検証や証明支援系の技術について勉強・研究したいと思っています。趣味の開発では、JavaScriptを用いてWebアプリを作ったり、Rustを用いてGtkアプリを作ったりと、できるだけ手を動かして、そのときに作りたいものを作っています。

関連 URL

KVSP(成果物)サイト：
https://github.com/virtualsecureplatform/kvsp
本人サイト：https://anqou.net/