IPA

2019 年度 未踏 IT 人材発掘・育成事業 採択案件評価書

1. 担当 PM

首藤 一幸（東京工業大学 情報理工学院 准教授）

2. クリエータ氏名

松岡航太郎（京都大学 工学部 電気電子工学科）
伴野良太郎（京都大学 工学部 情報学科）
松本直樹（京都大学 工学部 情報学科）

3. 委託金支払額

2,304,000 円

4. 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

5. 関連 Web サイト

https://github.com/virtualsecureplatform/kvsp

6. テーマ概要

暗号化されたままのデータを計算する手法・技術を、秘密計算という。準同型暗号を用いると秘密計算が可能だが、行える演算は加算と乗算に限られる。ただし、準同型暗号で可能な演算によって論理演算（例：1 NAND 0 → 1）が可能であり、論理演算が可能ということは、それを用いてプロセッサ・CPU の機能を組み上げることが可能ということである。本プロジェクトは、準同型暗号を用いてプロセッサの機能を組み上げ、エミュレートし、プロセッサが行うことのできる任意の処理について秘密計算を可能とするものである。

7. 採択理由

通常のプロセッサが行うことのできるあらゆる処理を秘密計算してやろう、というプロジェクトである。つまりは、処理を例えばクラウドで行う際に、クラウド側には一切処理内容を知られずに、しかし処理はしてもらえる、ということである。

明日、あさって、すぐに世の中で役に立つ、という種類のプロジェクトではないが、信用しなくても（あらゆる）処理を依頼できる未来を見せてくれると信じる。

8. 開発目標

準同型暗号の処理は大変重いため、プロセッサのエミュレートは今日のプロエッサと比較して大変遅いものとなる。それでも極力速くするため、エミュレート対象のプロセッサ（のゲート数）はコンパクトなものとしたい。そのため、プロセッサを新規に設計する。

必要となる様々なツールを開発する。例えば、プロセッサを論理演算のレベルで準同型暗号に置き換えるツールが必要である。また、CPU や GPU に対して準同型演算の処理を割り当てて実行するランタイムも必要である。

プログラムを、独自設計プロセッサの機械語で書かねばならないのでは、プログラマの負担が大きい。そこで、高級言語からのコンパイラを開発する。アセンブラの開発も必要である。言語としては C 言語をサポートする。

9. 進捗概要

9 月の時点で早くも全体が動作し始めた。それ以降も、貪欲に、より効率のよいプロセッサやランタイムの開発、将来を見据えての準同型暗号ライブラリの自前開発などを進めた。例えば、プロセッサの命令セットアーキテクチャ（ISA）は 3 つ、プロセッサ自体は 5 つ、ランタイム（実行エンジン）は 3 つ開発した。

10. プロジェクト評価

専門家によると、準同型暗号を用いて（高級言語プログラムの実行に耐える）汎用プロセッサをエミュレートできること自体は知られていたことであり、着想それ自体に新規性はない。しかし、それを本当にやってしまった人はこれまで誰もいなかった。開発があまりに大変だからであろう。このプロジェクトでは、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。

エミュレートされたプロセッサの現時点での性能は、とんでもなく低い。100 万円くらいする高速な GPU カード（NVIDIA 社 Tesla V100）を 1 基用いて 1 クロックあたり約 5.5 秒、8 基用いて 1.5 秒である。数万円のスマートフォンのプロセッサが数 GHz（10 の 9 乗 Hz）に達するこの時勢に、1,000 万円近くするマシンを使ってなんと 0.7Hz という冗談のような低性能である。搭載している RAM と ROM はわずか 512 バイトずつである。今日時点で実用になる性能ではない。

しかし、まず、世界で初めて実現してしまったことに意義がある。実装をもって実現できることを実証して、それがいかほどの性能となるのかを世に示した。

また、CPU や GPU の性能向上に伴って、今後、性能は向上していく。特に、本プロジェクトの準同型暗号ベースプロセッサは、ハードウェアが持つ並列性を容易にふんだんに活かせるため、逐次処理の性能が向上しなくなった今日～将来においても、通常のプロセッサと比べて非常に速く性能が向上していく。本プロジェクトについては、ムーアの法則は続く。また、専用ハードウェアの設計・開発というアプローチもある。準同型暗号の理論、実装の進展も性能向上に寄与するだろう。

11. 今後の課題

論文の執筆と発表