社会変革に向けた ICT 基盤強化　　2022 年度
2022 年度採択研究代表者　　年次報告書

穐山 空道

立命館大学 情報理工学部
准教授

アドレスの秘匿によるサイドチャネル攻撃に頑健な OS

研究成果の概要

2022 年度は (i) RowHammer 攻撃に対する既存防御手法の弱点、(ii) キャッシュ競合攻撃を防ぐ研究の安全性の主張の整理、(iii) 効率的にページのランダム割り当てを実現する手法の設計と実装を進めた。

(i) では RowHammer を防ぐ研究のうち、広く行われている電荷の貯め直しを追加で行う手法を調査した。調査の結果、(a) 確率的に追加貯め直しを行う手法では高密度で RowHammer に弱い現在・未来の DRAM でオーバーヘッドが大きくなりすぎる、(b) RowHammer 攻撃が起こっているかを判定し攻撃を受けている箇所のみ選択的に貯め直す手法では、高密度な DRAM では攻撃の影響範囲が広く発見が難しい、複雑な攻撃パターンにより回避される、という大きな欠点があることが分かった。これらから、広く行われている電荷の貯め直しの追加では RowHammer の根本防止はできないと結論した。

(ii) では既存のキャッシュ競合攻撃の対策を調査し、安全性の主張を 3 つのパターンに整理した。具体的なパターンは (a) キャッシュ競合の検知に利用する eviction set を作成できる確率が十分低いことを主張する、(b) 攻撃者の観測に関しある性質が満たされれば安全と仮定し、その性質を満たすことを形式手法で証明する、(c) 被攻撃者のメモリアクセスパターンと攻撃者の観測の間の相互情報量が 0 または十分小さいことを示す、である。これらの利点・欠点を整理し、本研究でも (c) を参考にすることが有望と結論した。

(iii) ではまず既存のページ割り当て手法の流用を検討したが、ランダム化には適さないと判断したため独自手法を考案した。本手法は全メモリページをブロックに分割しブロック内の空き状況のみを管理することで管理データを削減し、各ブロックからランダムにページを選択しフリーリストに接続することでユーザのメモリ確保要求時にはリストの先頭のみを見る。これらの工夫により既存の bitmap 方式とフリーリスト方式の両方の欠点を克服する。現在、ユーザ空間レベルでの実装およびランダム性の検証を進めている。