革新的コンピューティング技術の開拓　　2022 年度
2020 年度採択研究代表者　　年次報告書

塩見 準

大阪大学 大学院情報科学研究科
准教授

光集積回路で切り拓く次世代セキュアコンピューティング基盤

研究成果の概要

本年度は、耐タンパ性という観点から、電気電子方式の回路と光集積回路と同列に比較することを目的に、CMOS 集積回路から漏えいする電磁波強度の定量的モデル化を行った。モデル化の過程で、漏えい電磁波と集積回路の動作パラメータの間に、初等関数で説明可能な依存関係があることを発見し、その依存関係の検証および耐タンパ性を有する CMOS 暗号回路の設計手法の研究を行った。実チップ検証のために商用 180 nm を用いて発振回路を設計し、その漏えい電磁波と発振周波数の間に前述の依存関係を発見した。特に、動作電圧に対して漏えい電磁波がスーパーリニアに削減されることをモデルから予測でき、耐タンパ性を有する暗号回路の設計手法の検討を行った。このコンセプトを実回路に適用するため、動作電圧を自由に変更可能な実用暗号回路を試作した。次年度に実用暗号回路に対しても提案モデルの検証を行う。

光の位相変調だけで論理演算をすることで、耐タンパ性を有しながら演算を行える事実に注目し、安全に乱数を生成する回路方式を検討した。当該回路は、素子数に対して指数関数的に乱数を生成できるポテンシャルを有しており、光集積回路のボトルネックである実装効率を克服する可能性がある。シリコンフォトニクスチップ試作サービスを通し、そのプロトタイプ回路を試作した。現在製造段階にあり、次年度に測定評価を行う。

前年度に試作した位相演算論理ゲートが納品され、その測定環境の構築を行った。排他的論理和を演算する光論理ゲートに対し、位相検波を行うことで、出力光が意図通り変調できていることを実測で確認した。次年度にさらなる測定と検証を行う。

【代表的な原著論文情報】

1) 南口 和生, 御堂 義博, 三浦 典之, 塩見 準, “集積回路より漏えいする電磁波の電源電圧依存性モデル”, DA シンポジウム 2022, pp. 58-63, 2022 年 8 月.