安心・安全な超スマート社会に向けた光セキュアコンピューティング

Optical Secure Computing towards a Safe and Secure Super-smart Society

京都大学[1]，JST さきがけ[2]，○塩見 準[1,2]

Kyoto University[1], JST PRESTO[2], ○Jun Shiomi[1,2]

E-mail: shiomi-jun@vlsi.kuee.kyoto-u.ac.jp

チップ内でコヒーレント光を変調して演算する光集積回路は，従来の CMOS (Complementary Metal-Oxide-Semiconductor) 集積回路とは一線を画す物理原理で動作する．安心・安全な超スマート社会の実現に向けた，耐タンパー光セキュアコンピューティング技術の展望を述べる．

情報機器を支えるキーデバイスである CMOS 集積回路に対する脅威として，サイドチャネル攻撃が報告されている．サイドチャネル攻撃は，集積回路より漏えいする電磁波や電流消費を不正に解析する，もしくは電磁波やレーザーを照射して意図的に誤動作させることで，その内部情報（例えば暗号の鍵情報）を盗み見る攻撃である．暗号処理回路が用いる暗号アルゴリズム自体がいかに堅牢でも，サイドチャネルを通した攻撃で暗号鍵などの秘密情報を盗聴できる．暗号情報が飛び交う次世代の超スマート社会において，暗号処理プロセッサの内部状態を秘匿する能力(耐タンパー性)を高めることは，超スマート社会の持続的発展のために極めて重要である．

光集積回路技術の発展により，CMOS 集積回路を凌駕する高速性・省エネルギー性を有する光集積回路の実現可能性が急速に高まっている．本発表では，光集積回路技術の新しい展開先として，耐タンパーセキュアコンピューティングを切り拓く．まず，コヒーレント光が持つ波動特性の中に，論理情報を秘匿できることを述べる．従来の振幅変調ベースの光コンピューティング手法と異なり，図 1 (a)のように，位相変調をベースに論理演算をすることで，光信号強度を一定に保ちながら演算し，強靭な耐タンパー性を実現することを述べる．次に，位相論理情報の特有の性質 (周期性や多値性) について触れ, 集積ナノフォトニクス技術を例に位相論理ゲートや検波技術(図 1 (b))を述べて，耐タンパーコンピューティング技術へ展開する．最後に，超スマート社会を支えるセキュアコンピューティング技術としての，光集積回路技術の将来展望を議論する．

本研究は JST さきがけ (#JPMJPR20M3) の支援をうけたものである．

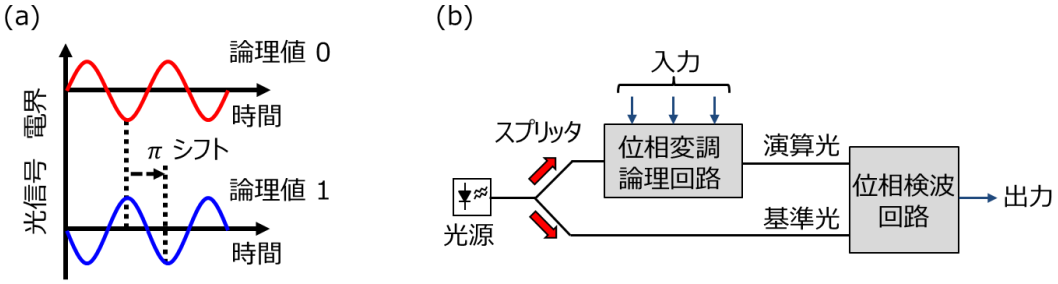

図 1: 光集積回路技術のセキュアコンピューティングへの展開．(a) 位相変調に基づく耐タンパー符号化．(b) 位相変調に基づく論理回路と検波回路．