

光ニューラルネットワークにおける 物理攻撃耐性のシミュレーション

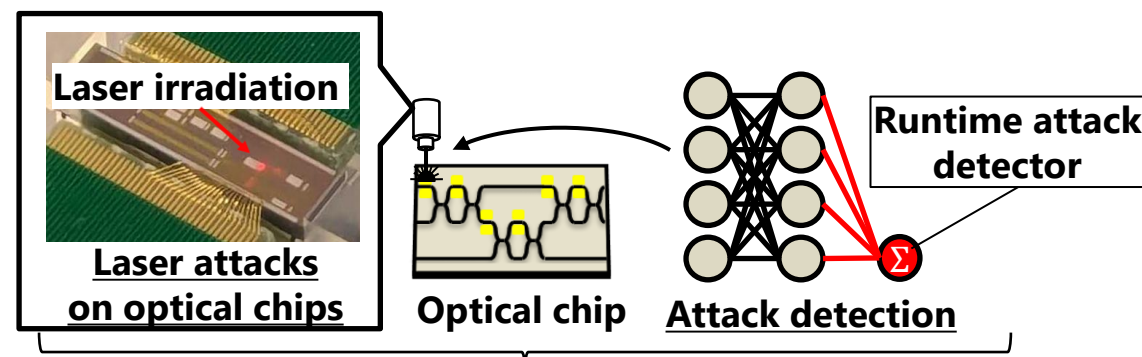
大阪大学大学院情報科学研究科 西田孔太、塩見準

目的 光の干渉を用いて高効率演算を行う光ニューラルネットワーク (ONN) に対する物理攻撃の耐性の評価、および物理攻撃への対策技術の開発

内容 光集積回路に対してレーザー照射を行い、ONNの重みパラメータを不正に書き換えることを狙う。この効果を再現するシミュレータをSQUID上で構築し、このレーザー故障注入攻撃によるニューラルネットワークの誤分類発生率、および攻撃の実行時検知率（異常検知用のチェックサムをONNに導入）をシミュレーションにより評価した。

結果 約96%の攻撃を実行時に検知できた

利用した計算機	SQUID GPUノード群
	ノード時間 5208 時間
	使用GPU数 8
	並列化 2 or 4ノード 並列



Attack simulation using **SQUID GPU nodes**

図（シミュレーション環境概要）