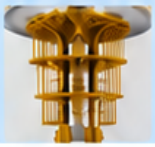
未来の暗号を、計算の中から守る
― ポスト量子暗号における乗算処理の防御技術 ―

背景　なぜ新しい暗号が必要なのか？

将来、量子コンピュータが実用化されると、
現在使われている公開鍵暗号の一部が
解読される可能性があります。
そこで注目されているのが、量子コンピュータ
でも破られにくい「ポスト量子暗号（PQC）」
です。



量子
コンピュータ
（将来の脅威）



→ ポスト
量子暗号
（PQC）

攻撃（課題）　計算中に攻撃を受けたら？

暗号は数学的に安全でも、実際の機器が
攻撃されることがあります。
例えば「故障注入攻撃」は、機器に物理的な
影響（電圧・電磁波・温度の変化など）を与え、
計算をわざと間違わせる攻撃です。
こうした誤りが、秘密情報を推測する手がかりに
なる場合があります。



故障注入攻撃
（物理的な影響で
計算を誤らせる）

研究の内容　暗号の「乗算」を守る

ポスト量子暗号では、大きな数の
乗算が繰り返し使われています。
その乗算が攻撃によって誤って計算
されても、異常を検出できる仕組み
（乗算の防御）を研究しています。



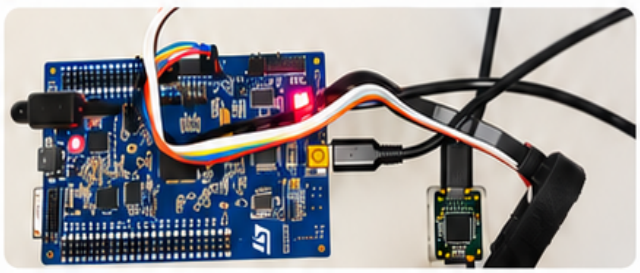
乗算とは？
2つの数を掛け合わせる計算です（例：3×4＝12）。
暗号では、非常に大きな数の乗算を繰り返し行います。

正常な乗算 → 故障注入 → 誤りの検出 → 安全性の確保

目標（実践）　実際の機器で、防御の効果を確かめる

研究した乗算の防御方法を、
実際の開発ボードに実装し、
攻撃による誤りを正しく検出できるかを
実験で確認します。
さらに、処理の性能も評価し、
安全性と実用性の両立を目指します。





研究の意義　この研究で、どんなことができる？



乗算に対する攻撃を検出できる仕組みを実現することで、
ポスト量子暗号を実際の機器で安心して利用できるようになります。
これにより、将来の量子コンピュータ時代でも、
安全な通信・認証・データ保護の基盤に貢献します。

- 暗号の信頼性を高める
- 実機で使える安全な実装を目指す
- 安全な社会基盤（通信・認証・データ保護）に貢献