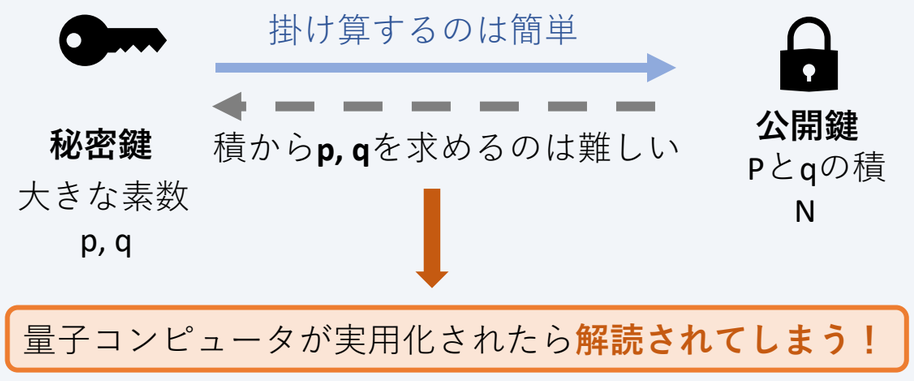
Kyberに対するスクリーミングチャネルの同時収集攻撃の検証

崎山·李·宮原 研究室

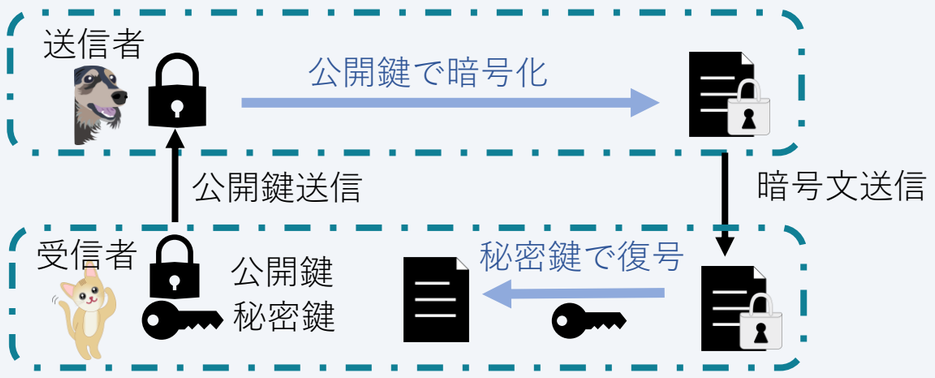
量子コンピュータと耐量子暗号

- 現在のRSA暗号などの公開鍵暗号は，量子コンピュータの実用化により解読されるリスクがある
- 米国国立技術研究所(NIST)は2024年夏に量子コンピュータ実用化に備えて耐量子暗号を選定した



公開鍵暗号

- ペアで生成される公開鍵と秘密鍵を使用する暗号
- 公開鍵で暗号化し，対応する秘密鍵で復号する
- 秘密鍵から公開鍵の計算は簡単(公開鍵は秘密鍵から作れる)
- 公開鍵から秘密鍵の逆計算は非常に困難である
- 公開鍵から秘密鍵が計算できたら**だれでも復号できてしまい**安全性が損なわれる



Kyberとは

2024年夏にNISTが標準化したLWE問題の困難性を利用した公開鍵暗号

LWE(Learning with Errors)問題

方程式に誤差を与えると次数が大きい場合解を求めるのが難しいという問題

$$\begin{bmatrix}4 & 3 & 1 & 5\\ 2 & 2 & 9 & 3\\ 1 & 5 & 0 & 7\\ 6 & 4 & 1 & 8\end{bmatrix}\begin{bmatrix}s_1\\ s_2\\ s_3\\ s_4\end{bmatrix}+\begin{bmatrix}e_1\\ e_2\\ e_3\\ e_4\end{bmatrix}=\begin{bmatrix}3\\ 9\\ 1\\ 8\end{bmatrix}$$

係数 **公開鍵**に相当　　未知定数 **秘密鍵**に相当　　誤差 (非公開)　　定数 **公開鍵**に相当

→ 誤差付きの方程式は**次数が多いと難しい**

研究内容

研究目的　**Kyberに対して複数周波数の漏洩電波を同時に収集する攻撃を行い，組み合わせることで秘密鍵の復元効率が向上するかを検証する**

実験方法

❶二つの測定器を用いて異なる二つの周波数の波形を同時に収集する

❷計算している値との相関値を取る(関係性を調べる)

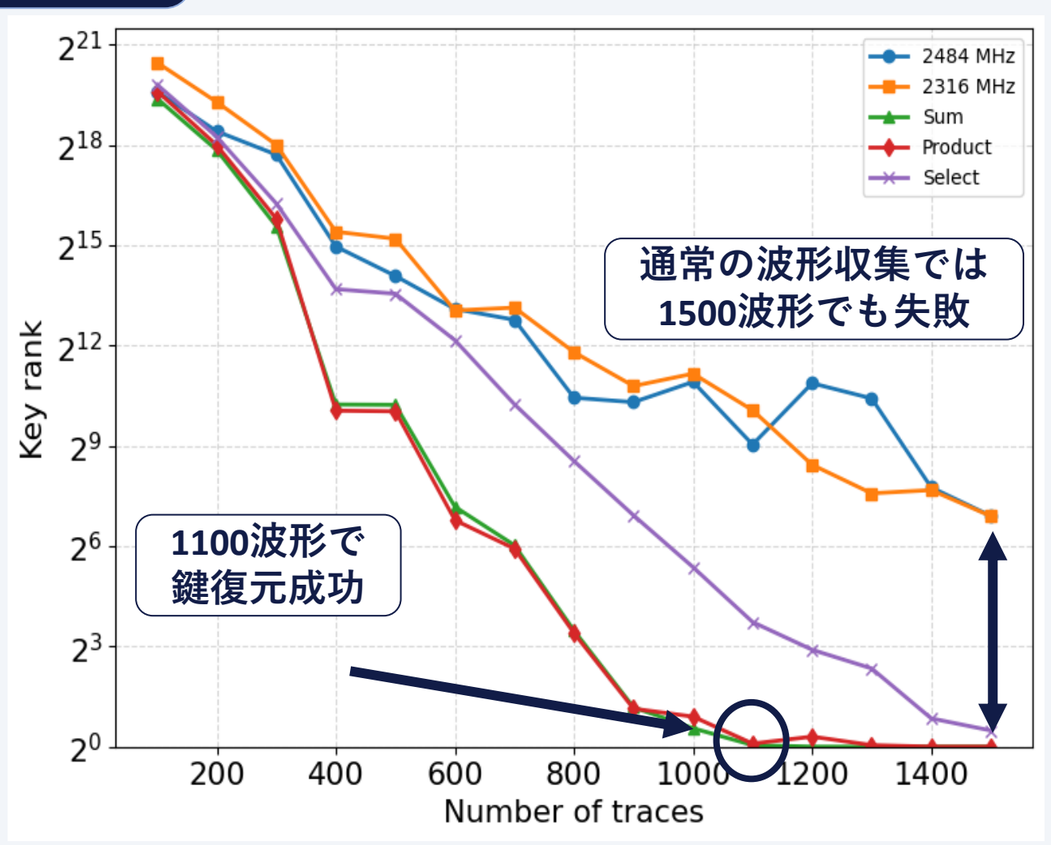
❸2つの周波数で得られた相関値組み合わせ，通常の鍵復元と秘密鍵の復元効率を比較する

実験結果

同時収集攻撃により，**より少ない波形数，暗号実行回数**による鍵復元に成功した

同時収集攻撃
1100波形
で鍵復元に成功

通常の波形収集
1500波形
でも失敗



鍵候補における正解鍵の相関係数の順位と波形数の関係
(下に行くほど鍵復元に近づく)

作成者: 室本悠生

崎山・李・宮原研究室HP
https://sakiyama-lab.jp/