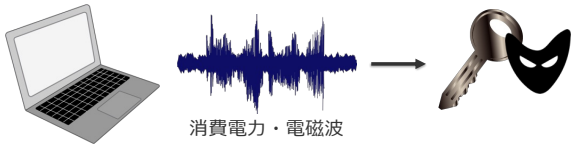
耐量子計算機暗号への サイドチャネル攻撃

崎山・李・宮原 研究室

研究概要

サイドチャネル攻撃とは、暗号を計算している機器から漏れる消費電力や電磁波の変化を手がかりに、中に隠された秘密鍵を推測する攻撃です。

暗号の数学的な安全性とは別に「どう実装したか」によって鍵が盗まれてしまうことがあります。



漏れた波形から**鍵**を取り出す

耐量子計算機暗号　量子コンピュータが実用化されると、いま広く使われている RSA 暗号などは解読されてしまいます。そこで量子コンピュータでも解くのが難しい「格子」の問題を使った新しい暗号が作られ、2024年に米国 NIST が署名方式 **ML-DSA** を標準化しました。

どこを狙うか　ML-DSA は計算を速くするために、多項式の掛け算を数論変換（NTT）で小さな掛け算に分けて行います。私が狙うのは、この途中で秘密の値と既知の値を掛ける部分です。

$$r = s_0 c_0 + s_1 c_1$$

s：秘密要素　**c**：既知要素
r：計算結果。**この値が漏洩する**

研究テーマ

問い：既存の攻撃手法 ZV-FA を、もっと速く確実に鍵復元するように改良できないか？

1 既存手法 ZV-FA のしくみ

$c_1 = 0$ になる波形だけを使うと式の後半が消え、調べる候補の組み合わせが 769×769 通りから 769 通りずつに減らせます。

$$r = s_0 c_0 + s_1 c_1$$
↓ $c_1 = 0$ の波形だけ使う
$$r = s_0 c_0$$

2 見つけた問題：「0」が見えない

秘密要素 s_0 が 0 だと、計算結果は常に 0 になり、波形との相関（似ている度合い）が計算できません。その結果、**本当は正解であるはずの 0 が候補の下位に沈んでしまいます。**

候補の順位（イメージ）

1位	312
2位	45
⋮	
下位	0 ← 本当の正解

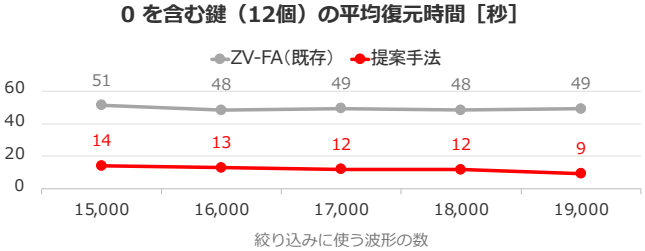
3 提案：0 を優先し、安い順に鍵列挙する

① 1位の相関が低い係数では、0 を最優先の候補にします。

② 各候補に「1位からどれだけ相関が下がるか」をコストとして付け、合計コストが小さい鍵から順に確かめます。

ZV-FA で候補を絞る
↓
0 を優先
↓
候補にコストを付ける
↓
安い鍵から順に検証
↓
鍵を復元

結果とこれから



計算機上のシミュレーションで、50 個の鍵を使って評価しました。

- 波形 19,000 本で、**50 個すべての鍵を復元**
- 0 を含む鍵では、約 50 秒 → **約 9〜14 秒** に短縮
- 0 を含まない鍵では既存手法と同程度

今後も手法の改良を試みており、さらに実際のマイコン（Arm Cortex-M4）で測った波形で効果を確かめます。

この成果は国際会議 WISA 2026 で発表しました。

制作者：蔵谷 陸