SCにおけるpqm4実装のKyberへの非プロファイル攻撃鍵復元実験

室本 悠生[1,a)]　宮原 大輝[1]　崎山 一男[1]　李 陽[1]

概要：量子コンピュータの実用化により現在広く用いられている RSA などの公開鍵暗号が破られる可能性が指摘されている．そのため NIST は，耐量子暗号の標準化に取り組んでおり，2024 年 8 月に CRYSTALS-Kyber を ML-KEM という名称で鍵カプセル化メカニズムとして標準化した．耐量子暗号に対するサイドチャネル攻撃の耐性は重要な研究課題であり，相関電力解析などの攻撃手法については多くの研究が進められている．一方で，Camurati らが提案したスクリーミングチャネルとは漏洩電磁波が無線通信部に混入することで無線電波として放射される漏洩である．これにより電磁波による攻撃よりも遠距離での攻撃が可能であることが示された．しかしながら Kyber に対してスクリーミングチャネルを用いた鍵復元を行った研究は少ない. 本研究では、ML-KEM として標準化された Kyber に対し，復号処理中の数論変換後の多項式乗算に対してスクリーミングチャネルによる鍵復元を行い，秘密鍵係数を抽出できることを示した．また，帯域幅・サンプリングレート・中心周波数帯といった波形収集パラメータを変化させながら測定を行うことで，漏洩の特性を評価した．

キーワード：耐量子暗号，スクリーミングチャネル，サイドチャネル攻撃

Non-profile attack key recovery experiment on pqm4 implementation of Kyber in SC

Yuki Muromoto[1,a)]　Daiki Miyahara[1]　Kazuo Sakiyama[1]　Yang Li[1]

Abstract: Due to the advancement of quantum computing, widely used public-key cryptosystems such as RSA are expected to become vulnerable. In response to this threat, NIST has launched a standardization project for post-quantum cryptography, and in August 2024, it standardized CRYSTALS-Kyber under the name ML-KEM as a key encapsulation mechanism.Resistance to side-channel attacks is a crucial concern in post-quantum cryptography, and numerous studies have been conducted on attack methods such as correlation power analysis. On the other hand, Screaming Channels, proposed by Camurati et al., are a novel class of side channels in which unintentional electromagnetic leakage is modulated and emitted as radio waves by on-chip wireless communication modules. This allows for attacks from greater distances compared to conventional electromagnetic side-channel attacks. However, there have been few studies that apply Screaming Channels to key recovery on Kyber. In this study, we target Kyber standardized as ML-KEM, and demonstrate that it is possible to extract secret key coefficients by performing key recovery using Screaming Channels, focusing on the polynomial multiplication that follows the Number Theoretic Transform (NTT) during decryption. Furthermore, we evaluate the leakage characteristics by varying waveform acquisition parameters such as bandwidth, sampling rate, and center frequency.

Keywords: Post-quantum Cryptography, Screaming Channels, Side-channel Attack

[1] 電気通信大学，東京都調布市調布ケ丘 1-5-1, The University of Electro- Communications, 1-5-1, Chofugaoka, Chofu, Tokyo, 182-8585, Japan
[a)] y.muromoto@uec.ac.jp

1. はじめに

近年量子コンピュータの実用化が進められており，従来の

RSA や楕円曲線暗号などの公開鍵暗号方式は破られる可能性が指摘されている．この脅威に対応するため，米国国立標準技術研究所 (NIST) は耐量子暗号 (Post-Quantum Cryptography: PQC) の標準化を進めており，2024 年の 8 月には 3 つの暗号方式が標準化された．鍵共有方式としては，格子ベースの CRYSTALS-Kyber が ML-KEM（Module-Lattice Key Encapsulation Mechanism）として選定され，署名方式としては同じく格子ベースの CRYSTALS-Dilithium が ML-DSA（Module-Lattice Digital Signature Algorithm）として採択された．さらに，ハッシュ関数を利用した電子署名である SPHINCS+が SLH-DSA(stateless-hash digital signing algorithm) として選定された．

暗号アルゴリズムは理論的には安全でも，ハードウェア上で動作させた場合には，電磁波や電力消費などの漏洩情報を利用した攻撃にさらされることがある．サイドチャネル攻撃とはこうした意図しない物理的な漏洩により秘密情報を抽出する攻撃であり，組込み機器や IoT デバイスによって脅威となる．さらに，近年では Camurati ら [3] が提案したスクリーミングチャネルと呼ばれる漏洩が報告されている．これは暗号計算時に生じる電磁波がアナログ回路に干渉することで無線信号として増幅・伝搬するものであり，従来の近接電磁解析と比較して遠距離からの観測が可能となることから，より深刻な脅威となっている．

これまでに提案されている Kyber に対するサイドチャネル攻撃の多くは，暗号文に意図的な変更を加える選択暗号文攻撃や，同一デバイスにおけるトレースを事前に収集して学習を行うプロファイリング攻撃である．暗号文に変更を加えた選択暗号文攻撃は，復号時の暗号文正当性検証や復号失敗回数の制限により防御できる場合がある．また，プロファイリング攻撃は同種のデバイスで大量のトレースを収集し学習を行う必要がある．これらの攻撃に対し，本研究では，正規の暗号文を対象とする非プロファイリング型攻撃に着目し，従来電力解析で実証されていた Mujdei ら [7] の NTT ドメインにおける多項式乗算をターゲットとした相関電力解析手法をスクリーミングチャネルに適用した．

攻撃対象には Nordic nRF52832 ARM Cortex-M4F System on Chip（SoC）を搭載した BLE Nano V2 を用い，pqm4 ライブラリ [6] で実装された Kyber の復号処理を対象に，10cm 離れた位置から電磁波を取得した．その結果，暗号化 500 回の平均化を行った波形を用いることで，最小 554 トレースで秘密鍵を復元できることを確認した．また，スクリーミングチャネルにおける大きな漏洩を観測できる中心周波数帯の探索を行い，鍵復元に必要なトレース数に大きな影響を与えることを明らかにした．加えて，鍵復元に必要なサンプリングレートおよび帯域幅の条件についても評価を行い，遠距離・非接触環境下における測定パラメータの指針を示した．

本稿の構成は以下の通りである．第 2 節では関連研究について述べる．第 3 節では Kyber やサイドチャネル攻撃の事前知識を説明する．第 4 節で実験環境と条件を述べ，第 5 節で今回の攻撃方法を示す．第 6 節で実験とその結果を示し，最後に第 7 節で結論と今後の研究を述べる．

2. 関連研究

Hamburg ら [5] は，Kyber の復号における逆数論変換を標的とした攻撃を提案した．攻撃者は特別に作成した暗号文を送り込み，逆数論変換の入力を多くの係数がゼロとなる形にして観測を容易にする．これにより途中の演算結果から秘密鍵の係数を推定し，最終的に鍵全体を復元できることを示した．実験では，少数回の観測で秘密鍵が復元可能であり，ノイズが大きい環境（標準偏差 2 以上）でも成功することが確認された．また，秘密鍵を 2 分割して処理する単純なマスク化では防御できないことも明らかにした．

Mujdei ら [7] は相関電力解析を用いた攻撃を提案した．彼らは有効な暗号文を入力し，復号処理中の多項式乗算における電力消費を観測して秘密鍵を推定する手法を示した．特に，Toom-Cook 法や数論変換（Number Theoretic Transform, NTT）を用いた乗算の演算結果に基づき，ハミングウェイトを漏洩モデルとする相関解析を行い，Kyber, Saber，NTRU に対して鍵復元を達成している．

スクリーミングチャネルを用いた攻撃に関しては，Wang ら [4] が Kyber を対象とする深層学習を用いたプロファイリング攻撃によるメッセージ復元を報告している．この攻撃は暗号文にエラーを注入し，暗号文 1 個を 255 通りに改変するマルチビットエラー注入法という手法を用いている，これにより攻撃セットを拡張することで，深層学習の分類精度を高めることで効率的なメッセージ復元をした．ただし，この手法は暗号文正当性検証により防御される可能性があり，さらに同一デバイスでの事前学習を必要とする．

これらに対し，本研究は，正規の暗号文を用い，事前学習やエラー注入を行わない非プロファイリング型のスクリーミングチャネル攻撃であり，NTT ドメインにおける多項式乗算をターゲットとする点に特徴がある．従来の電力解析手法を電磁漏洩に適用し，非接触かつ 10cm の距離から秘密鍵復元を実証した点で，既存研究とは異なる．

3. 前提知識

3.1 Kyber の概要

Kyber は Module-Learning With Errors(M-LWE) に基づいた鍵カプセル化メカニズム（Key Encapusulation Mecahism: KEM）である．

KEM とは公開鍵暗号方式を利用して，共通鍵暗号のための鍵を共有するためのプロトコルであり，鍵生成，公開鍵で暗号化し相手に送信するカプセル化，受信した暗号文から秘密鍵を使用して復号する復号化の 3 つの処理から構

成される．

M-LWE 問題は従来の Learning With Errors（LWE）問題を多項式環上のモジュール構造に拡張したものである．具体的には多項式環

$$R_q = \mathbb{Z}q[X]/f(X) \tag{1}$$

上のランク k のモジュール，すなわち

$$R_q^k = (\mathbb{Z}q[X]/f(X))^k \tag{2}$$

を扱う．これにより LWE 問題の秘密ベクトルや誤差ベクトルが多項式のベクトルに置き換えられ，それらと多項式係数の行列 $\mathbf{A}$ との積に誤差ベクトル $\mathbf{e}$ を加えた以下の関係式が成り立つ．

$$\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \pmod{q} \tag{3}$$

ここで $\mathbf{s} \in R_q^k$ は多項式ベクトルであり秘密鍵,$\mathbf{A} \in R_q^{k \times k}$,$\mathbf{b}$ は公開鍵に対応する．また $\mathbf{e} \in R_q^k$ は誤差を含む多項式ベクトルであり非公開情報である．

3.2 数論変換

数論変換（Number Theoretic Transform, NTT）は高速フーリエ変換を有限体や整数環上で定義したものである．Kyber をはじめとした格子暗号で，多項式の乗算の計算量削減を目的として用いられている．入力多項式の係数を $a_0, a_1, \ldots, a_{n-1}$，有限体上の原始根を ω とすると数論変換は次のように定義される．

$$\mathrm{NTT}(a)_k = A_k = \sum_{j=0}^{n-1} a_j \cdot \omega^{jk} \pmod{q} \tag{4}$$

多項式 $a(x) = \sum a_j x^j$ と $b(x) = \sum b_j x^j$ の積の係数 $c_k = \sum_{i=0}^{k} a_i b_{k-1}$ であり，直接計算した場合の計算量は $O(n^2)$ である．しかし数論変換したうえで乗算をすると係数ごとに計算できる．そのため数論変換を用いることで，計算量を直接計算時の $O(n^2)$ から $O(n \log n)$ へと計算量を大幅に削減することができる．

3.3 相関攻撃

相関攻撃とは漏洩モデルから作成した予測リーケージと収集したリーケージとの相関係数を利用して秘密鍵を推定するサイドチャネル解析の手法である．この相関攻撃のうちリーケージとして消費電力を用いる CPA(correlation Power Analysis) は Brier ら [2] によって提案された．攻撃者は既知の入力と秘密鍵候補から漏洩モデルを生成し，このモデルと実際に計測したリーケージとの間で相関係数を計算する．その結果，最も高い相関係数を示す鍵候補を真の秘密鍵であると推定する．

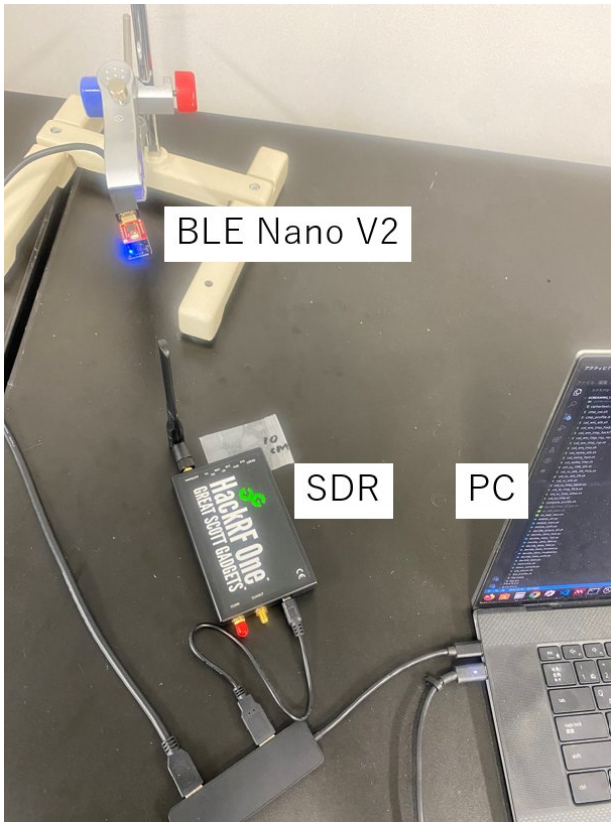

図 1 実験環境

3.4 スクリーミングチャネル

スクリーミングチャネルとは Camurati ら [3] が提案したミックスドシグナルチップで発生する，遠距離でも観測できるサイドチャネル情報である．ミックスドシグナルチップとは一つのチップにデジタル回路 (プロセッサ) とアナログ回路 (無線通信部) を搭載した SoC である．従来の電磁波による解析は，デバイスから漏れ出す電磁放射を近距離でとらえる手法であった．一方スクリーミングチャネルはプロセッサが生じる電磁波がアナログ回路に混入し，無線電波として発信される現象を利用する．この結果，機密情報が本来の無線通信信号とともに意図せず広範囲に漏洩し，攻撃者は物理的に離れた場所からでもサイドチャネル攻撃を行うことが可能となる．Camurati らは AES-128 に対して最大 15m の距離から鍵復元をし，漏洩は最大 60m で検出可能であることを示した．

4. 実験環境

波形採取環境は Camurati らの実験を参考に図 1 のように作成した．ターゲットデバイスは Nordic nRF52832 ARM Cortex-M4F System on Chip（SoC）を搭載した BLE Nano V2 を使用し，波形収集には HackRF を使用した．アンテナとターゲットデバイスの距離は 10cm とし，ノート PC でターゲットデバイス，SDR の操作を行った．トレー

Algorithm 1 KYBER.CPAPKE.Dec(sk, c): Decryption

Require: Secret key $sk \in B^{12\cdot k\cdot n/8}$, Ciphertext $c \in B^{d_u\cdot k\cdot n/8+d_v\cdot n/8}$

Ensure: Message $m \in B^{32}$

1: $u \leftarrow \mathrm{Decompress}_q(\mathrm{Decode}_{d_u}(c), d_u)$
2: $v \leftarrow \mathrm{Decompress}_q(\mathrm{Decode}_{d_v}(c + d_u \cdot k \cdot n/8), d_v)$
3: $\hat{s} \leftarrow \mathrm{Decode}(sk)$
4: $m \leftarrow \mathrm{Encode}_1(\mathrm{Compress}_q(v - \mathrm{NTT}^{-1}(\hat{s} \circ \mathrm{NTT}(u)), 1))$
5: **return** m

ス波形にはノイズが含まれるため, その影響を抑えるために平均化処理を行った．具体的には, 同じ暗号文を 600 回復号し, それぞれの波形を収集した後, その中から最大 500 回分の波形を重ねて平均を取り，1 本のトレースとした．暗号化は ARM Cortex M4 用に最適化された pqm4 ライブラリ [6] の Kyber512 を BLE Nano V2 に書き込んだ．

5. 攻撃方法

攻撃手法については Mujdei ら [7] の論文を参考にしたが，彼らの攻撃は消費電力に基づくものであるのに対し，本研究ではスクリーミングチャネルを用いた．ターゲットとするのは復号処理における NTT ドメインでの多項式乗算である．Algorithm 1 は公式ドキュメント [1] から引用した Kyber の復号アルゴリズムで，その 4 行目の $\hat{s}\circ\mathrm{NTT}(u)$ の計算を攻撃対象とする．

5.1 kyber におけるペア乗算

Kyber では NTT ドメインで多項式係数の 2 係数ごとの乗算が行われる．秘密鍵多項式 s と暗号文多項式 u に対して $N = 256$ の係数列を数論変換後にペア (a_{2i}, a_{2i+1}), u_{2i}, u_{2i+1} と分割し，各ペアごとに次式の演算を行う．

$$r_{2i} = u_{2i}s_{2i} + \zeta \cdot u_{2i+1}s_{2i+1} \pmod{Q} \tag{5}$$

$$r_{2i+1} = u_{2i}s_{2i+1} + u_{2i+1}s_{2i} \pmod{Q} \tag{6}$$

ここで ζ は事前計算された回転因子，法 $Q = 3329$ である．このペア乗算は $i = 0, 1, \ldots, 127$ の順で実行され，1 回の多項式乗算につき $N/2 = 128$ ペアが処理される．

5.2 pqm4 における乗算のアセンブリ実装

pqm4 における数論変換後の係数ペアごとの乗算のアセンブリコードを Listing 1 に示す．8 行目の命令でレジスタ tmp に係数 $r_{2i} = u_{2i}s_{2i} + \zeta \cdot u_{2i+1}s_{2i+1} \pmod{Q}$ が格納される．また 11 行目の命令でレジスタ tmp2 に係数 $r_{2i+1} = u_{2i}s_{2i+1} + u_{2i+1}s_{2i} \pmod{Q}$ が格納される．その後 13 行目の pkhtb 命令によって tmp，tmp2 の両方の値が 1 つの 32 ビットレジスタにまとめて格納される．そして最終的に 14 行目の str 命令によってこのレジスタの値がメモリに書き込まれる．

Listing 1. pqm4 におけるペアの乗算のアセンブリ

```
1  .macro doublebasemul_frombytes_asm rptr, bptr, zeta, poly0,
       poly1, poly3, tmp, tmp2, q, qa, qinv
2      ldr.w \poly0, [\bptr], #4
3      smulwt \tmp, \zeta, \poly1
4      smlabt \tmp, \tmp, \q, \qa
5      smultt \tmp, \poly0, \tmp
6      smlabb \tmp, \poly0, \poly1, \tmp
7      // a1*b1*zeta+a0*b0
8      plant_red \q, \qa, \qinv, \tmp
9      // r[0] in upper half of tmp
10     smuadx \tmp2, \poly0, \poly1
11     plant_red \q, \qa, \qinv, \tmp2
12     // r[1] in upper half of tmp2
13     pkhtb \tmp, \tmp2, \tmp, asr#16
14     str \tmp, [rptr], #4
15     ...
```

5.3 str 命令を対象とした相関解析

本研究では、Listing 1 の 14 行目で行われる乗算結果の 2 係数が str 命令により保存されることに着目し，これを相関解析のターゲットとする．漏洩モデルとしては，保存される値のハミング重みを用い，秘密鍵係数の推定を行う．

暗号文係数 (u_0, u_1) と秘密鍵係数 (s_0, s_1) の演算結果 (r_0, r_1) は式 (7)，(8) で表される．

$$r_0 = u_0s_0 + \zeta \cdot u_1s_1 \pmod{Q} \tag{7}$$

$$r_1 = u_0s_1 + u_1s_0 \pmod{Q} \tag{8}$$

str 命令により (r_0, r_1) が結合された状態で保存されるため，漏洩モデルは式 (9) のようにこれらのハミング重みの和を用いる．

$$\widehat{L}(s_0, s_1; u_0, u_1) = \mathrm{HW}_{16}(r_0) + \mathrm{HW}_{16}(r_1) \tag{9}$$

全トレース $t = 1, \ldots, T$ に対して，収集したリーケージ L_t と予測リーケージ $\widehat{L}_t(s_0, s_1)$ との Pearson の相関係数を式 (10) のように計算する．

$$\rho(s_0, s_1) = \frac{\sum_{t=1}^{T}(L_t - \overline{L})(\widehat{L}_t(s_0, s_1) - \overline{\widehat{L}})}{\sqrt{\sum_{t=1}^{T}(L_t - \overline{L})^2}\sqrt{\sum_{t=1}^{T}(\widehat{L}_t(s_0, s_1) - \overline{\widehat{L}})^2}} \tag{10}$$

最終的な推定鍵ペアは，相関係数が最大となるものであり

$$(\hat{s}_0, \hat{s}_1) = \underset{s_0, s_1 \in (-Q/2, Q/2]}{\arg\max} |\rho(s_0, s_1)| \tag{11}$$

により決定される．

なお, 暗号文係数 (u_0, u_1) は攻撃者が任意に選択可能で既知であると仮定し, 保存される演算結果 (r_0, r_1) は秘密鍵係数 (s_0, s_1) に依存するため, 相関解析ではこれら 2 係数を同時に推定する必要がある．pqm4 では秘密鍵係数は法 Q に

対して中心化された範囲に制限され，$s_0, s_1 \in (-Q/2, Q/2]$ と定義される．Kyber では $Q = 3329$ のため，各係数の候補は 3329 通りとなり，秘密鍵候補の全組み合わせは $3329^2 = 11082241$ 通りとなる．

5.4 PoI の決定

サイドチャネル解析において，採取した波形のうち全てのサンプルポイントに漏洩があるわけではない．多くの場合，大きな漏洩が含まれるのは限られた時刻のみであり，これらの漏洩の大きいサンプルポイントを Point of Interest (PoI) と呼ぶ．PoI の選択は解析効率や鍵復元精度に直結する．

原理的には，全サンプルポイントに対して相関係数を計算し，最も高い相関値を与える鍵候補を推定鍵として決定することも可能である．しかしこの方法では，各サンプルポイントごとに鍵候補の相関係数を計算する必要があり，計算時間がかかる．

そこで本研究では，計算量削減のために，既知の秘密鍵を用いたプロファイリング段階を設け，相関係数が最大となる時刻を PoI として特定した．未知鍵推定においては，この PoI 付近を解析対象とする．図 2 に示すように，既知鍵で算出した相関係数の時系列プロファイルには顕著なピークが観測され，そのピーク位置を PoI として採用した．この PoI は秘密鍵そのものには依存せず，同一の実装および同種のデバイスにおいては常に同一である．したがって，一度 PoI を決定すれば，以後の未知鍵推定でも共通して利用することが可能となる．

6. スクリーミングチャネルによる鍵復元実験

鍵復元の精度や効率は，取得する信号の品質に大きく依存する．そこで，中心周波数・サンプリングレート・帯域幅といった受信設定を変化させ，それぞれの条件下での復元性能を比較することで，受信パラメータが攻撃結果に与える影響を調べた．なお，基本的な測定条件としては中心周波数を 2.272GHz，サンプリングレートを 9MHz，帯域幅を 8MHz に設定し，解析対象のパラメータのみを変更して評価を行った．

6.1 中心周波数

Camurati らの論文 [3] によると，スクリーミングチャネルによる漏洩は f_{chan} を Bluetooth の周波数帯 (2.4GHz)，f_{chan} をターゲットデバイスの動作周波数とすると $f_{chan} \pm n \cdot f_{clock}$ で確認されている．今回のターゲットデバイスである BLE Nano V2 の動作周波数は 64MHz のため，ノイズの影響が小さく，復号を確認することのできた 2.272GHz(2.4GHz - $2 \cdot 64$MHz), 2.528GHz(2.4GHz + $2 \cdot 64$MHz)，2.592GHz(2.4GHz + $3 \cdot 64$MHz) の 3 つの中心周波数で 500 波形ずつ使用トレース数を増やしながら鍵復元を行った．

6.1.1 結果と考察

結果を図 3 に示す．縦軸は $Q^2 = 3329^2 = 11082241$ のうちの正解鍵の相関値の順位で，横軸がトレース数である．鍵復元効率は 2.272GHz，2.528GHz，2.592GHz の順に高かった．2.272GHz，2.528GHz はそれぞれ 1500 波形，7500 波形で鍵復元できた一方，2.592GHz は正解鍵は上位になったが 1 位になることはなかった．この結果から中心周波数の設定が鍵復元効率に非常に大きな影響を与えることが分かった．

6.2 サンプリングレート

サンプリングレートはアナログ信号をデジタル信号へ変換する際の標本化周波数であり，これが高いほど波形の時間分解能が高い．高いサンプリングレートを用いると，より細かい時間変化を観測することが可能となり，漏洩をより精密に捉えられる可能性がある．しかしその一方で，サンプリングレートが高いほど 1 波形あたりのサンプル数が増加し，データサイズや計算コストが大きくなるという欠点がある．逆にサンプリングレートを低くするとデータ量は削減できるが，信号の重要な変動を十分に捉えられず，必要波形数が増加する可能性がある．したがって，サイドチャネル解析においては，対象デバイスの動作速度や波形収集環境に応じて，効率と精度の両面から最適なサンプリングレートを選択することが重要となる．

本研究ではサンプリングレートを 5MHz, 6MHz, 7MHz, 8MHz, 9MHz に変更してそれぞれ 500 波形ずつ使用トレース数を増やしながら鍵復元を行った．

6.2.1 結果と考察

結果を図 4 に示す．7MHz 以上ではトレース数を増やせば安定して正解鍵が 1 位となった．9MHz が正解鍵が 1 位になるのに必要なトレース数が 1500 と 1 番少なく，続いて 8MHz の 3000 トレース，7MHz の 4000 トレースとなった．また，9MHz は 1500 トレース以降正解鍵はずっと 1 位だが，7MHz，8MHz は正解鍵が 2 位になるときがあった．一方，5MHz，6MHz は正解鍵の順位が安定しなかった．5MHz は正解鍵の順位は最大 608 位と上位になることはあったが，1 位には 1 回もならなかった．6MHz は 4000 トレースで 1 位となったが，5000 トレース以降正解鍵の順位は下がっていった．

この結果から，サンプリングレートが高いほど鍵復元に必要なトレース数は下がり，鍵復元の成功率も高くなることが分かった．また，サンプリングレートが少なすぎる場合，トレース数を増加させても正解鍵が 1 位になるとは限らないことが示唆された．これは，サンプリングレートが低いことで信号中の特徴的な情報が十分に取得できず，相関計算の精度が著しく低下するためと考えられる．6MHz では一時的に 1 位となったものの，以降は順位が低下し

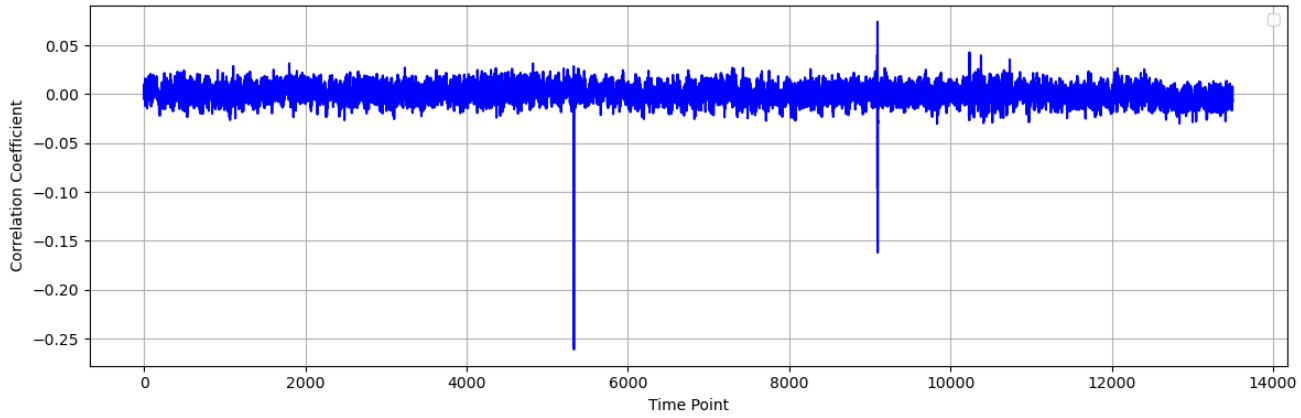

図 2　既知鍵における相関値

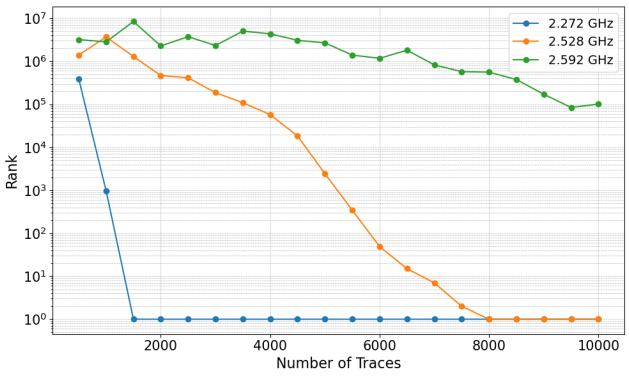

図 3　中心周波数と鍵復元効率

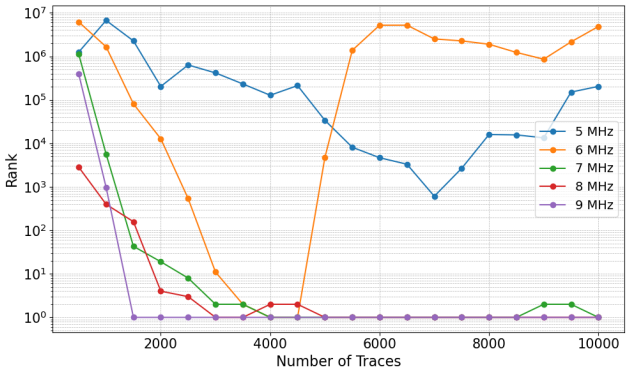

図 4　サンプリングレートと鍵復元効率

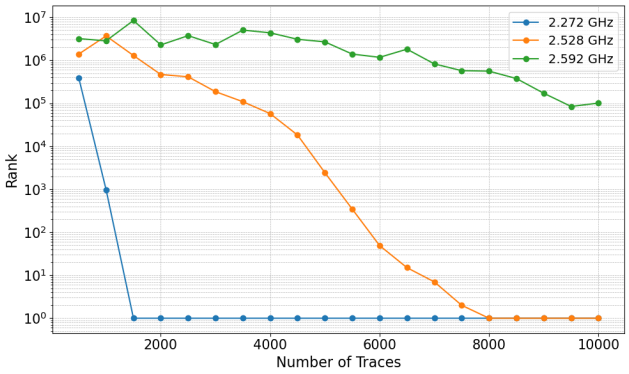

図 5　帯域幅と鍵復元効率

た．この結果からサンプリングレートが不十分な状態では、トレース数を増やしても復元精度が安定しないことが分かった．

6.3　帯域幅

帯域幅は観測機器が取り込む周波数成分の範囲を決定するパラメータである．広い帯域幅を設定すると信号成分を多く含めることができるが，同時にノイズも多く取り込む可能性がある．一方で帯域幅を狭めるとノイズは減少するが，漏洩がとらえられず，復元効率が低下する場合がある．

本研究ではサンプリングレートを 6MHz，7MHz，8MHz に変更してそれぞれ 500 波形ずつ使用トレース数を増やしながら鍵復元を行った．

6.3.1　結果と考察

結果を図 5 に示す．7MHz，8MHz ではいずれも 1000 トレースで正解鍵が 1 位となった．一方で 6MHz では 10000 トレースまで試行しても正解鍵は徐々に上位にはなったものの，1 位には達しなかった．また 7MHz と 8MHz を比較すると，7MHz の方が鍵復元効率が良かった．この原因として，7〜8MHz 付近には有効なサイドチャネル漏洩成分が少なく，広帯域化によってその範囲の不要な成分や外来ノイズを取り込んでしまい，信号対雑音比（SNR）が低下した可能性がある．一方で 7MHz では，復号に有効な周波数成分を十分確保しつつ，不要な帯域のノイズ取り込みを抑えられたため，最も高い復元効率を示したと考えられる．

6.4　鍵復元に必要な最小トレース数

実験 6.3 の中心周波数 2.272GHz，サンプリングレート 8MHz，帯域幅 7MHz の結果がこれまでの実験の中で最も高い鍵復元効率を示した．そこで，帯域幅 7MHz の条件において，鍵復元に必要な最小トレース数の評価を行った．具体的には，使用トレース数を 500 トレースから開始し，1 トレースずつ増加させながら鍵復元を実施した．

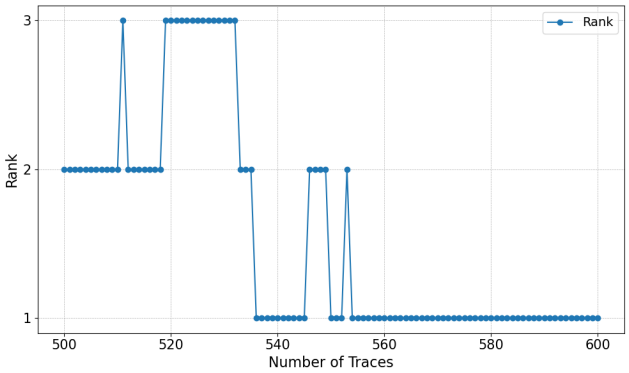

図 6 1 トレースごとの鍵復元結果

6.4.1 結果と考察

結果を図 6 に示す．鍵ランクが 1 位になった最小のトレース数は 536 トレース, 安定して鍵ランクが 1 位になったのは 554 トレース目からだった．例えば，図 3 を見ると中心周波数を 2.2528GHz に設定した場合，正解鍵が安定して 1 位になるまでに約 8000 トレースを必要としたことから，鍵復元に必要なトレース数は中心周波数や帯域幅などのパラメータ調整によって大きく変動することが確認できた．これらのパラメータはデバイスや環境条件ごとに異なる可能性が高いため, 効果的な鍵復元を実現するには, 事前に対象デバイスの特性を調査し，最適なパラメータ設定の調整が重要である．また，パラメータの調整が困難な場合にはこれよりも多数のトレースを収集する必要があると考えられる．

7. 結論と今後の研究

本研究では, 耐量子暗号として標準化された Kyber（ML-KEM）に対し，スクリーミングチャネルを用いた非プロファイリング型の鍵復元攻撃を実施した．具体的には，復号処理中の数論変換後の多項式乗算におけるペア演算を対象とし，pqm4 実装を搭載した ARM Cortex-M4 デバイスから 10cm の距離で漏洩信号を取得，相関解析によって秘密鍵係数の推定に成功した．

実験の結果，最適なパラメータ（中心周波数 2.272GHz，サンプリングレート 8MHz，帯域幅 7MHz）を選択した場合，554 トレースで鍵復元を達成できることを確認した．さらに，中心周波数，サンプリングレート，帯域幅といった波形取得条件が鍵復元効率に大きな影響を与えることを示し，スクリーミングチャネル攻撃における計測パラメータ選定の重要性を明らかにした．

今後は相関電力解析に加えて，単純電力解析など，ほかのサイドチャネル解析の手法をスクリーミングチャネルに適用可能かどうかを検討したい．また，今回は NTT ドメインの乗算結果のハミングウェイトを漏洩モデルとして使用したが，より高精度な漏洩モデルを検討することで，鍵復元に必要なトレース数の削減をしたい．

謝辞 本研究は, JST 経済安全保障重要技術育成プログラム【JPMJKP24U2】の支援を受けたものです．

参考文献

[1] Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS–Kyber: acca-secure module-lattice-based kem. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 353–367, London, UK, April 2018.

[2] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. *International workshop on cryptographic hardware and embedded systems*, pages 16–29, 2004.

[3] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018.

[4] Y. Chang, Y. Yan, C. Zhu, and P. Guo. Template attack of lwe/lwr-based schemes with cyclic message rotation. *Entropy*, 24(10):1489, October 2022.

[5] Mike Hamburg, Julius Hermelink, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine Vredendaal. Chosen ciphertext k-trace attacks on masked cca2 secure kyber. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 88–113, 08 2021.

[6] Matthias J. Kannwischer, Joost Rijneveld, Peter Schwabe, and Ko Stoffelen. Pqm4: Post-quantum crypto library for the arm cortex-m4. `https://github.com/mupq/pqm4`. Accessed: 2025-08-15.

[7] Catinca Mujdei, Lennert Wouters, Angshuman Karmakar, Arthur Beckers, Jose Mera, and Ingrid Verbauwhede. Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication. *ACM Transactions on Embedded Computing Systems*, 23, 11 2022.