HQC に対する OT-PCA 攻撃の成功率を予測する理論モデル

YAN XIN　（指導教員：李 陽 准教授）
電気通信大学 情報理工学域 II類 セキュリティ情報学プログラム

① 研究背景：なぜ HQC の安全性を調べるのか

量子計算機に耐える暗号が必要
耐量子暗号（PQC）の標準化が進行中。**HQC** は**誤り訂正符号**に基づく PQC で、2025 年に NIST が標準化対象に選定。

誤り訂正の「上限」が手がかりになる　※ 50 個・1001 は説明用の例

訂正できる | 失敗

1 0 0 1 → 失敗 → 1 1

訂正できる誤りの数には**上限**がある（例：50 個）
成功・失敗が半々になる**誤りパターン**（例：1001）を入れる
失敗なら、パターンが 0 の位置の鍵は**1 の可能性が高い**

実装の安全性も評価が必要
機器の動作から漏れる情報（**サイドチャネル**）で「復号の**成功／失敗**」が分かると、秘密鍵を絞り込める。これが **OT-PCA 攻撃** [1]。

安全性を正しく評価するには、この攻撃が設計・設定次第でどこまで成功するかを知る必要がある
これまで成功率は、設定を変えるたびにシミュレーションで調べていた

② 先行研究：OT-PCA 攻撃のしくみ　— 「復号の成功／失敗」から鍵を 0 らしい順に並べ、先頭を 0 とみなして解く

秘密鍵 (x, y)（約 35,000 ビット中、1 は約 130 個） → ① 問い合わせ（誤りパターンで成功／失敗を観測） → ② テンプレート（各ビットが 1 である確率） → ③ 確率順にソート（0 らしい順に並べる） → ④ ISD で鍵を解く（探索パラメータ T_0, T_1, w_0, ℓ）

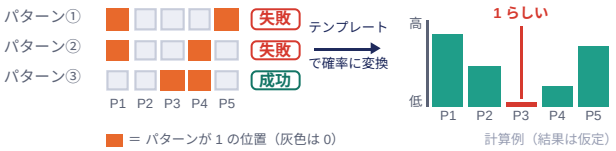
前段：設計（精度 ρ・問い合わせ回数 t・誤りパターン）で決まる　　後段：探索パラメータで変わる

1 誤りパターンを混ぜて問い合わせる。誤りパターン e を入れた暗号文を復号させ、**成功か失敗か**を観測する。復号の途中の値は：

計算の中間値　$v - u\cdot y = mG + (x\cdot r_2 - y\cdot r_1 + e)$

成否は括弧内の **1 の個数**で決まり、それは**鍵 x, y** によって変わる。

2 成功／失敗を「0 らしさ」に変換する。鍵の 1 が、パターンが 0 の位置にあると失敗しやすく、1 の位置にあると成功しやすい。この関係の表（**テンプレート**）で、複数パターンの結果を**掛け合わせて 0 らしさ**を得る。



P3 が 1 なら、パターンが 0 の ①② では誤りが増えて失敗、
パターンが 1 の ③ では誤りが減って成功 → 観測と合うので「P3 は 1 らしい」

3 0 らしい順に並べ、先頭を 0 とみなして鍵を解く（ISD）。（下図：左ほど 0 らしい、｜＝真の 1）



成功条件：0 と認定した T_1 個に 1 がなく、残りの各半分で 1 が w_0 個以下

探索パラメータ

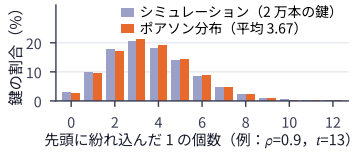
T_0	0 可能性が最大のビットを上位から選択する数
T_1	その T_0 個のうち，0 と認定するビット数
w_0	残りのビットにおいて，1 として許容するビット数
ℓ	探索範囲の拡張長

先頭に紛れ込んだ 1 が少ないほど、攻撃は成功しやすい。その数は**前段の設計**で、どこまでを 0 とみなすかは**探索パラメータ**で決まる。

③ 本研究：成功率を予測する理論モデル　— 設計と設定から、シミュレーションなしで成功率を計算する

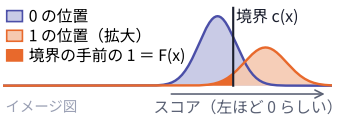
前段の設計（精度 ρ・問い合わせ回数 t・誤りパターン・テンプレート） → ② 完全解析（鍵を作らずに計算） → $F(x)$（並べ替えた先頭 x 個に紛れ込む 1 の平均個数） → ① 後段理論（ポアソン分布 ＋ 探索パラメータ） → **成功率**（シミュレーションなしで予測できる）

① 後段理論：成功率は $F(x)$ の 2 つの値で決まる



- 鍵の 132 個の 1 は小さな確率（約 2.8%）で先頭に紛れ込む → **少数の法則**で個数は**ポアソン分布**
- 必要なのは $F(T_0)$，$F(n+\ell)$ の 2 つだけ

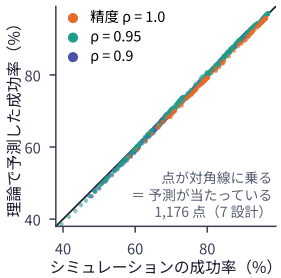
② 完全解析：鍵を作らずに $F(x)$ を計算



- 問い合わせはブロックごと → **1 ブロックを調べれば十分**
- 中身と応答の出方を**確率つきで数え上げ**、分布を求める
- 境界より手前の 1 の平均 ＝ $F(x)$

④ 成果と意義　— 予測は正確で、パラメータの最適化もシミュレーションなしでできる

主成果 予測はシミュレーションと一致する

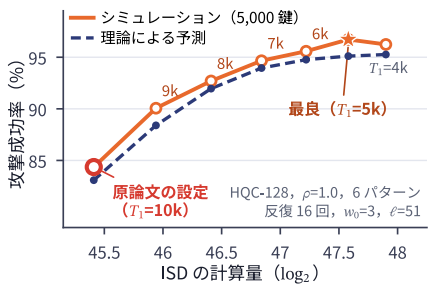


最大 1.6 ポイント
予測とシミュレーションの差
（7 設計・1,176 点）

最大 0.26 ポイント
理論で選んだ最適 T_0 の損失

数秒 ／ 約 5 分
1 設定の計算時間
（理論 ／ シミュレーション）

応用 パラメータの最適化も、シミュレーションなしで



- 理論はシミュレーションと**同じ形**の曲線を描き、最良の T_1（4k〜5k 付近）も一致（差は最大 2.0 ポイント）
- 原論文の設定から最適化すると **84.4% → 96.7%（+12.4 ポイント）**。計算量は約 4.5 倍
- 理論だけでも 83.1% → 95.3%（+12.2 ポイント）と予測

意義 原論文の設定だけで評価すると、攻撃の強さを**過小評価**しうる。理論なら最適化した攻撃の強さを**数秒**で見積もれるので、対策の効果確認など HQC の**安全性評価**に使える。（シミュレーションと理論に基づく見積もりで、実機での攻撃実験ではない）

まとめ
- 設計と設定から成功率を予測する**理論モデル**を構築
- 予測はシミュレーションと**最大約 2 ポイント以内**で一致
- 最適化で成功率 **+12.4 ポイント**（84.4% → 96.7%）

今後
- 計算量（ISD）まで含めた最適設定を理論で求める
- 異なる精度 ρ・SoftStern 型への適用

参考文献 [1] H. Dong and Q. Guo, “OT-PCA: New Key-Recovery Plaintext-Checking Oracle Based Side-Channel Attacks on HQC with Offline Templates,” IACR TCHES, vol. 2025, no. 1, pp. 251–274, 2025.