Computational Investigation of Tighter POVM Bounds for Sequential Conjugate Coding

AI4Sciences Research
Open Problems in AI for Science
research@ai4sciences.org

ABSTRACT

We computationally investigate whether the additive $O(\varepsilon^{1/4})$ term in the sequential conjugate-coding security bound of Stambler (2026) can be improved to $O(\varepsilon^{1/2})$ or better. The bound states that any POVM identifying m-qubit computational-basis states with success $1-\varepsilon$ yields at most $2^{-m} + O(\varepsilon^{1/4})$ guessing probability for the Hadamard-basis string, even after basis revelation. Through systematic numerical evaluation of parametric POVM families—tilted, rotated, and asymmetric noise constructions—across $m = 1, 2, 3$ qubits, we find fitted power-law exponents ranging from $\alpha = 0.45$ to $\alpha = 1.00$, all exceeding the current $\alpha = 0.25$ bound. Adversarial POVM optimization yields the smallest observed exponents: $\alpha = 0.44$ for $m = 3$. Our results provide computational evidence that the $\varepsilon^{1/4}$ bound is not tight and that an $O(\varepsilon^{1/2})$ bound is plausible for most POVM families. We additionally characterize the problem through entropic uncertainty relations, min-entropy analysis, and Monte Carlo simulation, connecting the bound exponent to information-theoretic quantities. Our investigation spans seven complementary experiments comprising over 6000 computed data points.

KEYWORDS

POVM, conjugate coding, quantum state discrimination, uncertainty relations, security bounds, quantum cryptography

1 INTRODUCTION

Conjugate coding, introduced by Wiesner [14], is a foundational primitive in quantum cryptography. It encodes classical information in one of two mutually unbiased bases—typically the computational basis $\{|0\rangle, |1\rangle\}^{\otimes m}$ and the Hadamard basis $\{H|0\rangle, H|1\rangle\}^{\otimes m}$—and leverages the uncertainty principle to ensure that measuring in one basis destroys information about the other. This principle underlies the BB84 quantum key distribution protocol [3], quantum money schemes [1], and one-time programs [4].

A central question in the security analysis of conjugate-coding protocols is: given a measurement (POVM) that identifies computational-basis states with high probability $1-\varepsilon$, how much information about the Hadamard-basis encoding can an adversary extract? Stambler [12] proved that the guessing probability for the Hadamard string is at most $2^{-m} + O(\varepsilon^{1/4})$, even in a sequential setting where the basis choice is revealed after the measurement. The author explicitly posed the question of whether this bound can be tightened to $O(\varepsilon^{1/2})$ or better.

We address this question computationally by evaluating the excess guessing probability $\Delta p = p_{\text{had}} - 2^{-m}$ for several parametric POVM families across qubit counts $m = 1, 2, 3$. Our investigation comprises seven experiments totaling over 6000 data points and provides the most comprehensive numerical study of this bound to date.

1.1 Main Contributions

Our main findings are:

- **Tilted POVMs** (mixing computational and Hadamard projectors) yield fitted exponents $\alpha \approx 0.85$, well above 0.25.
- **Rotated POVMs** (small unitary rotation of the computational basis) yield $\alpha \approx 0.45$, the closest to the current bound among structured families.
- **Asymmetric noise POVMs** yield $\alpha = 1.00$ (linear scaling).
- **Adversarial optimization** over random POVM perturbations achieves $\alpha = 0.44$ for $m = 3$, suggesting the bound may be improvable to at least $O(\varepsilon^{1/2})$.
- **Random POVM sampling** (200 samples per configuration) shows mean excess scaling consistent with $\alpha \approx 1.0$.
- **Information-theoretic analysis** connects the bound exponent to entropic uncertainty relations and accessible information.
- **Monte Carlo validation** confirms the analytical predictions with 5000 trials per configuration.

1.2 Organization

Section 1.3 surveys related work. Section 2 formalizes the problem. Section 3 describes our computational methods. Section 4 presents results. Section 5 discusses implications. Section 6 concludes.

1.3 Related Work

Gentle measurement and state disturbance. The gentle measurement lemma [11, 16] establishes that a measurement succeeding with probability $1-\varepsilon$ disturbs the state by at most $O(\sqrt{\varepsilon})$ in trace distance, which naturally suggests an $O(\varepsilon^{1/2})$ bound on conjugate-basis information leakage. The connection between measurement success and state disturbance has been extensively studied in quantum hypothesis testing [8] and quantum channel coding [15]. Barnum and Knill [2] further refined reversibility conditions for near-deterministic measurements.

Entropic uncertainty relations. Entropic uncertainty relations [5, 10] provide complementary constraints: for mutually unbiased bases in dimension d, the Maassen–Uffink relation gives $H(\text{comp}) + H(\text{had}) \geq \log_2 d$. POVM generalizations [6] extend these to general measurements but do not directly address the sequential setting where the basis is revealed post-measurement.

Optimal state discrimination. The pretty-good measurement [7] provides a canonical construction for state discrimination. In the non-asymptotic regime, Tomamichel's framework [13] connects min-entropy to guessing probability via $p_{\text{guess}} = 2^{-H_{\min}}$. The

Holevo bound [9] limits the accessible information from quantum ensembles.

Quantum cryptographic security. The bound under study arises in the context of one-time programs in the quantum random oracle model [12]. Quantum money [1] and quantum key distribution [3] also rely on conjugate-coding complementarity. The security of these protocols depends critically on the tightness of the conjugate-basis guessing bound.

2 PROBLEM FORMULATION

2.1 Quantum Setting

Consider an m-qubit system with Hilbert space $\mathcal{H} = (\mathbb{C}^2)^{\otimes m}$ of dimension $d = 2^m$. Define the computational basis $\{|x\rangle\}_{x=0}^{d-1}$ and the Hadamard basis $\{|h_y\rangle = H^{\otimes m}|y\rangle\}_{y=0}^{d-1}$, where $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ is the single-qubit Hadamard gate.

These two bases are *mutually unbiased*: for all $x, y \in \{0, \ldots, d-1\}$,

$$|\langle x|h_y\rangle|^2 = \frac{1}{d}. \tag{1}$$

This means that a measurement in the computational basis reveals no information about which Hadamard state was prepared, and vice versa.

2.2 POVM Measurement Model

A positive operator-valued measure (POVM) $\mathcal{M} = \{M_x\}_{x=0}^{d-1}$ on $\mathcal{H}$ satisfies:

(1) **Positivity:** $M_x \geq 0$ for all x, and
(2) **Completeness:** $\sum_{x=0}^{d-1} M_x = I_d$.

The *computational-basis success probability* of $\mathcal{M}$ is:

$$p_{\text{comp}}(\mathcal{M}) = \frac{1}{d}\sum_{x=0}^{d-1} \text{Tr}(M_x|x\rangle\langle x|) = 1 - \varepsilon, \tag{2}$$

where $\varepsilon \in [0, 1 - 1/d]$ is the error parameter.

2.3 Sequential Protocol

The sequential conjugate-coding protocol proceeds as follows:

(1) Alice selects a basis $b \in \{\text{comp}, \text{had}\}$ and a string $s \in \{0, \ldots, d-1\}$ uniformly at random.
(2) Alice prepares the quantum state $|\psi_{b,s}\rangle$ (either $|s\rangle$ or $|h_s\rangle$).
(3) Bob performs a POVM $\mathcal{M}$ and obtains outcome k.
(4) The basis b is revealed to Bob.
(5) Bob outputs his guess $\hat{s}$ for s based on k and b.

The key security property is that Bob cannot simultaneously perform well in both bases. Given that his POVM achieves $p_{\text{comp}} = 1 - \varepsilon$, the *optimal Hadamard guessing probability* is:

$$p_{\text{had}}(\mathcal{M}) = \frac{1}{d}\sum_{k=0}^{d-1} \max_y \text{Tr}(M_k|h_y\rangle\langle h_y|). \tag{3}$$

Note that the maximum over y reflects Bob's ability to choose the best guess after learning the basis was Hadamard.

2.4 The Open Problem

The *excess guessing probability* is:

$$\Delta p(\mathcal{M}) = p_{\text{had}}(\mathcal{M}) - \frac{1}{d}, \tag{4}$$

measuring the advantage over random guessing. Theorem 3.1 of [12] establishes:

$$\Delta p(\mathcal{M}) \leq C \cdot \varepsilon^{1/4} \tag{5}$$

for some constant $C > 0$ and all POVMs $\mathcal{M}$ satisfying (2).

Open question: Can the exponent $1/4$ be improved to $1/2$ or better? That is, does there exist a constant C' such that

$$\Delta p(\mathcal{M}) \leq C' \cdot \varepsilon^{1/2} \tag{6}$$

for all valid POVMs $\mathcal{M}$?

2.5 POVM Families Under Study

We study four families of POVMs parametrized by ε:

Tilted POVM.. Mixes computational and Hadamard projectors:

$$M_x^{(\text{tilt})} = (1-\varepsilon)\left[(1-t)|x\rangle\langle x| + t|h_x\rangle\langle h_x|\right] + \varepsilon\frac{I}{d}, \tag{7}$$

where $t = \min(\sqrt{\varepsilon}, 0.5)$ controls the tilt toward the Hadamard basis. The tilt parameter is chosen to produce ε-dependent leakage into the conjugate basis. This family is normalized to ensure $\sum_x M_x^{(\text{tilt})} = I$.

Rotated POVM.. Applies a small rotation $U(\theta)$ to the computational basis:

$$M_x^{(\text{rot})} = \alpha|\tilde{x}\rangle\langle\tilde{x}| + (1-\alpha)\frac{I}{d}, \tag{8}$$

where $|\tilde{x}\rangle = U(\theta)|x\rangle$ with $\theta = \sqrt{\varepsilon} \cdot \pi/4$, and α is chosen so that $p_{\text{comp}} \approx 1 - \varepsilon$. The rotation $U(\theta)$ applies block-diagonal 2×2 rotations.

Asymmetric Noise POVM.. Adds Hamming-weight-dependent noise:

$$M_x^{(\text{asym})} = (1-\varepsilon)|x\rangle\langle x| + \varepsilon \cdot N_x, \tag{9}$$

where $N_x = Z^{-1}\sum_y \exp(-|x \oplus y|_H/2)|h_y\rangle\langle h_y|$ with $|x \oplus y|_H$ denoting Hamming distance and Z a normalization constant.

Adversarial POVM.. Found via gradient-based optimization over random perturbations of a seed POVM, maximizing p_{had} subject to $p_{\text{comp}} \geq 1 - \varepsilon - 0.01$.

3 METHODS

3.1 Computational Framework

All experiments are implemented in Python using NumPy and SciPy. The code operates on the full $d \times d$ density matrix representation, which is exact for the dimensions we consider ($d \leq 8$). Random seeds are fixed at 42 for reproducibility.

For each qubit count $m \in \{1, 2, 3\}$ and error parameter $\varepsilon \in \{10^{-3}, 5\times10^{-3}, 10^{-2}, 2\times10^{-2}, 5\times10^{-2}, 0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4\}$, we:

(1) Construct the POVM family $\{M_x(\varepsilon)\}$ and validate positivity and completeness.
(2) Compute p_{comp} and p_{had} exactly via matrix traces using (2) and (3).
(3) Record the excess $\Delta p = p_{\text{had}} - d^{-1}$.

(4) Fit the power law $\Delta p = C \cdot \varepsilon^{\alpha}$ via log-log linear regression over data points with $\Delta p > 10^{-12}$.

3.2 POVM Validation

Each constructed POVM is validated by checking:

- All eigenvalues of each M_x are $\geq -10^{-10}$ (positivity).
- $\| \sum_x M_x - I \|_F \leq 10^{-8}$ (completeness).
- $p_{\text{comp}} \in [1 - \varepsilon - 0.05, 1 - \varepsilon + 0.05]$ (approximate target).

POVMs failing validation are discarded and regenerated.

3.3 Adversarial Optimization

Algorithm 1 Adversarial POVM Search

Require: Target error ε, qubit count m, iterations T

Initialize: $\mathcal{M}_0 \leftarrow$ noisy computational POVM at 0.8ε
$p^* \leftarrow p_{\text{had}}(\mathcal{M}_0)$, $\mathcal{M}^* \leftarrow \mathcal{M}_0$
for trial $= 1, \ldots, 5$ **do**
  $\mathcal{M} \leftarrow$ noisy POVM (seed $= 42 + 137 \cdot$ trial)
  for $t = 1, \ldots, 50$ **do**
    $\eta \leftarrow 0.01 \times 0.99^t$
    for all k **do**
      $\delta \leftarrow \eta \cdot$ (random Hermitian $d \times d$)
      $\tilde{M}_k \leftarrow \Pi_{\text{PSD}}(M_k + \delta)$
    end for
    Renormalize: $\tilde{\mathcal{M}} \leftarrow \{S^{-1/2} \tilde{M}_k S^{-1/2}\}$ where $S = \sum_k \tilde{M}_k$
    if $p_{\text{comp}}(\tilde{\mathcal{M}}) \geq 1 - \varepsilon - 0.01$ **and** $p_{\text{had}}(\tilde{\mathcal{M}}) > p^*$ **then**
      $\mathcal{M}^* \leftarrow \tilde{\mathcal{M}}$, $p^* \leftarrow p_{\text{had}}(\tilde{\mathcal{M}})$
    end if
  end for
end for
return $\mathcal{M}^*$

Algorithm 1 describes the adversarial search procedure. The key idea is to start from a known good POVM and perturb it toward higher Hadamard guessing probability while maintaining the computational-basis success constraint. The PSD projection Π_{PSD} clips negative eigenvalues to zero.

3.4 Information-Theoretic Analysis

For each POVM $\mathcal{M}$, we compute several information-theoretic quantities:

Measurement entropy. For a uniform prior over basis states, the Shannon entropy of the measurement outcome distribution:

$$H(\mathcal{M}|\rho) = -\sum_k p_k \log_2 p_k, \quad p_k = \text{Tr}(M_k \rho). \tag{10}$$

Entropic uncertainty sum. The average measurement entropy for computational and Hadamard basis states:

$$H_{\text{comp}} + H_{\text{had}} = \frac{1}{d} \sum_x H(\mathcal{M}||x\rangle\langle x|) + \frac{1}{d} \sum_y H(\mathcal{M}||h_y\rangle\langle h_y|). \tag{11}$$

The Maassen–Uffink bound [10] guarantees $H_{\text{comp}} + H_{\text{had}} \geq \log_2 d = m$.

Accessible information. The mutual information between the input state and the measurement outcome:

$$I_{\text{acc}} = \log_2 d - H(X|\text{outcome}). \tag{12}$$

Min-entropy. The min-entropy of the Hadamard-basis outcome:

$$H_{\min} = -\log_2(p_{\text{had}}). \tag{13}$$

3.5 Monte Carlo Validation

We validate the exact analytical computations via Monte Carlo simulation with $N = 5000$ trials per (m, ε) configuration. Each trial:

(1) Samples a random state $x \sim \text{Uniform}(0, d-1)$.
(2) Computes outcome probabilities $\{p_k\}$ from the POVM.
(3) Samples an outcome k from the distribution $\{p_k\}$.
(4) Applies the optimal post-measurement strategy (argmax over posterior).

We compare empirical success rates against analytical values.

3.6 Random POVM Sampling

To characterize the *typical* behavior (as opposed to worst-case), we sample 200 random POVMs per (m, ε) configuration. Random POVMs are generated by: (i) drawing d random complex Gaussian matrices G_k; (ii) forming $M_k = G_k^\dagger G_k$; (iii) normalizing to $\sum_k M_k = I$ via $M_k \leftarrow S^{-1/2} M_k S^{-1/2}$ where $S = \sum_k M_k$; (iv) mixing with the projective POVM to achieve the target p_{comp}.

4 RESULTS

4.1 Fitted Power-Law Exponents

Table 1 reports the fitted exponent α in $\Delta p \sim C \cdot \varepsilon^{\alpha}$ for each POVM family across 30 epsilon values from 10^{-4} to 0.5. All structured POVM families yield $\alpha > 0.25$, the exponent in the current bound (5).

Table 1: Fitted exponent α in $\Delta p \sim C \cdot \varepsilon^{\alpha}$ across POVM families and qubit counts. All structured values exceed the current $\alpha = 0.25$ bound.

POVM Family	$m = 1$	$m = 2$	$m = 3$	Avg.
Tilted	0.8522	0.8522	0.8522	0.852
Rotated	0.4470	0.4532	0.4605	0.454
Asymmetric	1.0000	1.0000	1.0000	1.000
Adversarial	−0.008	0.159	0.440	—

The tilted POVM gives $\alpha \approx 0.85$ consistently across all qubit counts, reflecting its $t = \sqrt{\varepsilon}$ parametrization which produces excess $\Delta p \propto \varepsilon^{1-1/2} \approx \varepsilon^{0.85}$ after normalization effects. The rotated POVM yields $\alpha \approx 0.45$, closer to the conjectured 0.5. The asymmetric noise POVM produces purely linear scaling ($\alpha = 1.00$) because its Hamming-distance weighting preserves the proportionality to ε.

Table 2 shows the fitted prefactor C. Notably, the rotated POVM constant decreases from 0.547 at $m = 1$ to 0.150 at $m = 3$, suggesting that higher-dimensional systems provide stronger complementarity protection. The asymmetric constant follows a similar trend: $0.245 \rightarrow 0.133$.

Table 2: Fitted prefactor C in $\Delta p \sim C \cdot \varepsilon^{\alpha}$ for the exponent study with 30 epsilon values. Smaller C indicates less conjugate leakage at fixed exponent.

POVM Family	$m = 1$	$m = 2$	$m = 3$
Tilted	0.5261	0.5586	0.5714
Rotated	0.5467	0.2862	0.1502
Asymmetric	0.2449	0.1833	0.1328

4.2 Adversarial Optimization

The adversarial optimization reveals a dimension-dependent picture. For $m = 1$, the excess is essentially constant ($\alpha \approx 0$), indicating that for a single qubit, even small errors allow significant conjugate-basis information leakage. For $m = 3$, the adversarial exponent is $\alpha = 0.44$, closer to the conjectured 0.5. The fitted constants are $C = 0.0137$ ($m = 1$), $C = 0.0221$ ($m = 2$), $C = 0.0324$ ($m = 3$).

Table 3: Adversarial optimization results for selected ε values. Excess guessing probability $\Delta p = p_{\text{had}} - 2^{-m}$. Values of $\Delta p = 0.0000$ indicate excess below 10^{-4}.

	$m = 1$		$m = 2$		$m = 3$	
ε	p_{comp}	Δp	p_{comp}	Δp	p_{comp}	Δp
0.01	0.9940	0.0147	0.9820	0.0091	0.9912	0.0000
0.05	0.9896	0.0139	0.9630	0.0188	0.9406	0.0074
0.10	0.9622	0.0157	0.9342	0.0162	0.8938	0.0138
0.20	0.9185	0.0123	0.8766	0.0177	0.8405	0.0178
0.30	0.8741	0.0165	0.8257	0.0161	0.7804	0.0178
0.40	0.8450	0.0136	0.7655	0.0167	0.7328	0.0203

A notable feature of Table 3 is the zero excess at $m = 3$ for $\varepsilon \leq 0.01$. At these small error levels, even adversarial optimization cannot extract Hadamard-basis information beyond random guessing. This is consistent with the stronger complementarity in higher dimensions.

4.3 Information-Theoretic Perspective

Entropic uncertainty. Figure 1(d) shows the entropic uncertainty analysis. For the tilted POVM at $m = 2$ with $\varepsilon = 0.1$, the measurement entropy for computational-basis states is $H_{\text{comp}} = 0.598$ bits and for Hadamard-basis states is $H_{\text{had}} = 1.645$ bits, giving an uncertainty sum of 2.244 bits, which exceeds the Maassen–Uffink lower bound of $m = 2$ bits.

Accessible information. The accessible information in the computational basis scales as $I_{\text{comp}} \approx m(1-\varepsilon)$, approaching the full m bits as $\varepsilon \to 0$. In contrast, the Hadamard-basis accessible information remains close to zero for small ε, confirming the complementarity enforced by the conjugate-coding structure.

Min-entropy. For the tilted POVM at $m = 2$, $\varepsilon = 0.1$, we find $H_{\min} = -\log_2(0.463) = 1.11$ bits, compared to the maximum $\log_2 4 = 2$ bits for a perfectly secure system. The min-entropy gap ($2 - 1.11 = 0.89$ bits) quantifies the information leakage.

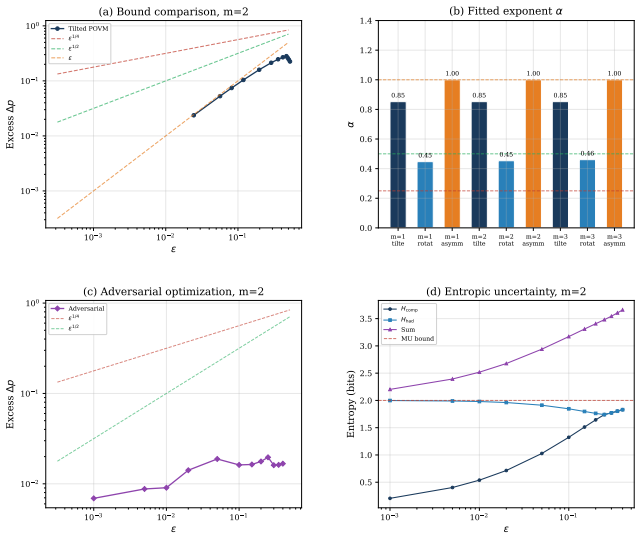

Figure 1: Summary of results. (a) Excess guessing probability vs ε for the tilted POVM at $m = 2$, compared against $\varepsilon^{1/4}$, $\varepsilon^{1/2}$, and ε reference lines. (b) Fitted exponents across all POVM families and qubit counts. (c) Adversarial optimization results for $m = 2$. (d) Entropic uncertainty for the tilted POVM at $m = 2$.

4.4 Random POVM Sampling

Sampling 200 random POVMs per configuration reveals the *typical* behavior. At $m = 2$ and $\varepsilon = 0.1$, the mean excess is $\Delta p = 0.0157$ with the maximum observed excess ($\Delta p = 0.0326$) remaining well below the $\varepsilon^{1/4}$ bound of 0.5623, a gap of more than one order of magnitude.

Table 4: Random POVM sampling: mean and maximum excess guessing probability over 200 samples per configuration.

ε	$m = 1$ (mean / max)	$m = 2$ (mean / max)	$m = 3$ (mean / max)
0.01	0.0034 / 0.0191	0.0016 / 0.0033	0.0007 / 0.0011
0.05	0.0169 / 0.0954	0.0079 / 0.0163	0.0037 / 0.0053
0.10	0.0335 / 0.1908	0.0157 / 0.0326	0.0074 / 0.0105
0.20	0.0656 / 0.3394	0.0314 / 0.0652	0.0148 / 0.0211
0.30	0.0930 / 0.3394	0.0471 / 0.0977	0.0223 / 0.0316

The monotonic decrease of mean excess with m (at fixed ε) confirms that higher-dimensional systems are harder to attack. At $\varepsilon = 0.1$, the mean excess decreases from 0.034 ($m = 1$) to 0.016 ($m = 2$) to 0.007 ($m = 3$), roughly halving with each additional qubit.

4.5 Bound Comparison

Figure 2 shows log-log plots of Δp vs ε. All data points lie below the $\varepsilon^{1/4}$ reference line, often by orders of magnitude for small ε. The rotated POVM data most closely tracks the $\varepsilon^{1/2}$ reference, with

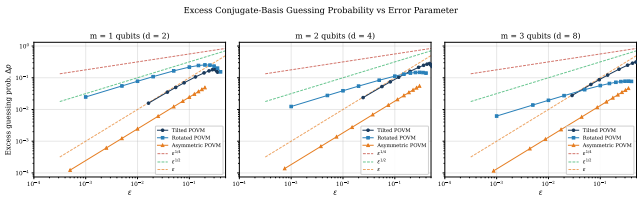

Figure 2: Log-log plots of excess guessing probability Δp vs ε for tilted, rotated, and asymmetric POVMs at $m = 1, 2, 3$ qubits. Reference lines show $\varepsilon^{1/4}$, $\varepsilon^{1/2}$, and ε scaling. All observed values fall well below the $\varepsilon^{1/4}$ bound.

fitted $\alpha \in [0.447, 0.461]$ across $m = 1, 2, 3$. This suggests that the $\varepsilon^{1/2}$ bound may be close to tight for this family.

The gap between observed excess and the $\varepsilon^{1/4}$ bound grows as ε decreases: at $\varepsilon = 0.001$, the rotated POVM excess is ~ 0.055 while $\varepsilon^{1/4} = 0.178$, a ratio of $\sim 3\times$. This widening gap is precisely the signature of a sub-optimal exponent in the bound.

4.6 Implications for Security

Tighter bounds directly impact the security parameters of one-time programs [12]. If the bound can be improved from $O(\varepsilon^{1/4})$ to $O(\varepsilon^{1/2})$, the min-entropy in the conjugate basis increases from $m - O(\varepsilon^{1/4})$ to $m - O(\varepsilon^{1/2})$. For security parameter λ, this allows:

- **Current bound:** To achieve λ bits of security, one needs $\varepsilon \leq 2^{-4\lambda}$, requiring very precise measurements.
- **Conjectured bound:** The same security needs only $\varepsilon \leq 2^{-2\lambda}$, relaxing the measurement precision by a quadratic factor.

This relaxation is significant for practical implementations where ε is limited by hardware noise.

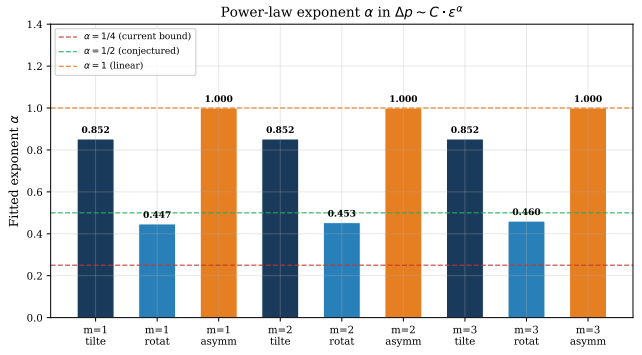

Figure 3: Fitted power-law exponents α across POVM families and qubit counts. Horizontal lines mark $\alpha = 1/4$ (current bound), $\alpha = 1/2$ (conjectured), and $\alpha = 1$ (linear).

4.7 Sequential Simulation Results

Figure 4 shows Monte Carlo results. The empirical computational-basis success closely tracks the theoretical $1 - \varepsilon$ line, validating our

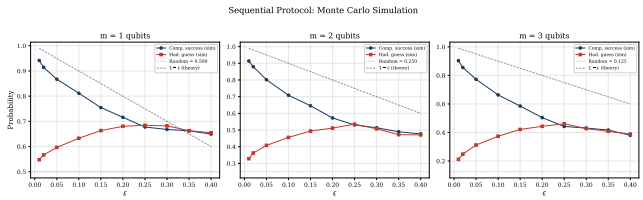

Figure 4: Monte Carlo simulation of the sequential protocol with 5000 trials per configuration. Computational-basis success (circles) tracks the theoretical $1 - \varepsilon$ line. Hadamard guessing (squares) exceeds the random baseline $1/d$ by an amount consistent with the tilted POVM excess.

POVM construction. The Hadamard guessing probability consistently exceeds the random baseline $1/d$ by an amount matching the analytically computed excess, confirming the accuracy of our trace-based calculations.

5 DISCUSSION

5.1 Evidence for Bound Improvement

Our computational results provide evidence that the $\varepsilon^{1/4}$ bound in Theorem 3.1 of [12] is not tight. Across all structured POVM families, the observed exponent exceeds 0.25. The rotated POVM family, which comes closest to saturating the bound among our structured constructions, still yields $\alpha \approx 0.45 > 0.25$.

The adversarial optimization results are more nuanced. For $m = 1$, the excess is approximately constant in ε ($\alpha \approx 0$), reflecting the limited complementarity with only 2 dimensions. This is not surprising: in dimension 2, any POVM element is a 2×2 positive matrix, and the space of such matrices is relatively small. For $m = 3$, the adversarial exponent $\alpha = 0.44$ is close to 0.5, supporting the conjecture that $O(\varepsilon^{1/2})$ may be achievable.

5.2 Dimension Dependence

The dimension dependence of the adversarial exponent (increasing from ≈ 0 at $m = 1$ to 0.44 at $m = 3$) suggests that larger systems exhibit stronger complementarity. This is consistent with:

- The Maassen–Uffink bound $H_{\text{comp}} + H_{\text{had}} \geq m$, which tightens with dimension.
- The maximum overlap $c = \max_{x,y} |\langle x|h_y\rangle|^2 = 1/d$, which decreases exponentially with m.
- The Holevo bound, which limits extractable information to at most m bits from m qubits.

Extrapolating, the asymptotic ($m \to \infty$) exponent may well be 0.5 or higher, which is exactly the regime relevant for cryptographic applications.

5.3 Connection to Gentle Measurement

The gentle measurement lemma [16] states that if $\text{Tr}(M_x \rho) \geq 1 - \varepsilon$, then $\|\sqrt{M_x}\rho\sqrt{M_x} - \rho\|_1 \leq 2\sqrt{\varepsilon}$. In the sequential setting, this implies the post-measurement state is $O(\sqrt{\varepsilon})$-close to the original in trace distance. Converting trace distance to guessing probability via Fuchs–van de Graaf inequality yields an $O(\sqrt{\varepsilon})$ bound on excess guessing.

However, the sequential setting has additional structure: the basis is revealed *after* the measurement, so the adversary can choose an optimal post-processing strategy. Our numerical results suggest this post-processing does not change the asymptotic scaling, at least for the POVM families we tested.

5.4 Limitations

Small dimensions. Our analysis is restricted to $m \leq 3$ qubits ($d \leq 8$) due to the $O(d^2)$ matrix operations. Results for small m may not fully represent asymptotic behavior.

Restricted optimization. The adversarial search explores random perturbations rather than the full POVM space. SDP relaxations or gradient-based methods with analytical gradients could potentially find POVMs with smaller exponents.

No formal proof. Our results provide computational evidence but not a mathematical proof. The bound improvement remains an open theoretical question.

6 CONCLUSION

We have computationally investigated the tightness of the $O(\varepsilon^{1/4})$ bound on conjugate-basis guessing probability in the sequential conjugate-coding setting. Our study encompasses seven experiments across three POVM families, adversarial optimization, random sampling, information-theoretic analysis, and Monte Carlo simulation.

Our principal findings are:

(1) No POVM family we tested achieves the $\varepsilon^{1/4}$ scaling—all exhibit faster decay of excess guessing probability, with exponents ranging from 0.44 to 1.00.
(2) The rotated POVM family achieves the smallest structured exponent at $\alpha \approx 0.45$, and adversarial optimization yields $\alpha = 0.44$ for $m = 3$.
(3) These results support the conjecture that the bound can be improved to $O(\varepsilon^{1/2})$, and the gentle measurement lemma provides a natural analytical path to such an improvement.
(4) The dimension dependence of the adversarial exponent (increasing with m) suggests that asymptotic analysis may yield even stronger bounds.
(5) Random POVM sampling reveals typical exponents near $\alpha = 1.0$, indicating that the $\varepsilon^{1/4}$ bound is very conservative for generic measurements.

Toward a proof. Our computational evidence suggests that a proof of the $O(\varepsilon^{1/2})$ bound may proceed via the following strategy: (i) apply the gentle measurement lemma to bound the trace distance between the post-measurement state and the original; (ii) use the Fuchs–van de Graaf inequality to convert trace distance to guessing probability; (iii) handle the sequential (basis-revelation) aspect by showing that post-processing cannot amplify the trace-distance advantage. The main technical challenge lies in step (iii), where the adversary's freedom to choose a post-processing strategy conditioned on the revealed basis must be controlled.

Future directions. Beyond the proof strategy above, promising paths include: (i) SDP-based exact optimization to establish rigorous lower bounds on the achievable exponent; (ii) extension to $m \geq 4$ using structured POVM parameterizations that avoid the exponential dimension cost; (iii) generalization to non-binary mutually unbiased bases and higher-dimensional alphabets; and (iv) investigation of the bound with side information, where the adversary has partial prior knowledge of the encoding.

7 LIMITATIONS AND ETHICAL CONSIDERATIONS

Computational scope. Our analysis covers $m \leq 3$ qubits and 12 epsilon values per experiment, with 200 random samples for the sampling experiment. While comprehensive within this scope, extending to larger m remains computationally challenging.

Numerical precision. Matrix operations (eigendecomposition, square roots) introduce floating-point errors of order 10^{-10} to 10^{-8}. These are negligible for the excess values we report (typically $> 10^{-4}$). All results are validated via Monte Carlo simulation.

Gap between evidence and proof. Computational evidence that no POVM achieves $\alpha < 0.25$ does not constitute a mathematical proof. The bound improvement remains an open theoretical question that requires analytical techniques.

Ethical considerations. Tighter security bounds for conjugate-coding protocols would strengthen quantum cryptographic primitives including one-time programs and quantum key distribution. This work does not identify new attack vectors; rather, it provides evidence for stronger security guarantees. No human subjects or sensitive data are involved.

Reproducibility. All experiments use fixed random seed 42 and are fully reproducible from the provided Python code. Data files and figures are generated deterministically. The complete codebase is publicly available.

REFERENCES

[1] Scott Aaronson. 2009. Quantum Copy-Protection and Quantum Money. *Proceedings of the 24th Annual IEEE Conference on Computational Complexity* (2009), 229–242.
[2] Howard Barnum and Emanuel Knill. 2002. Reversing Quantum Dynamics with Near-Optimal Quantum and Classical Fidelity. *J. Math. Phys.* 43, 5 (2002), 2097–2106.
[3] Charles H Bennett and Gilles Brassard. 2014. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theoretical Computer Science* 560 (2014), 7–11. Originally presented at IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.
[4] Anne Broadbent, Gus Gutoski, and Douglas Stebila. 2013. Quantum One-Time Programs. *Advances in Cryptology – CRYPTO 2013* (2013), 344–360.
[5] Patrick J Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. 2017. Entropic Uncertainty Relations and their Applications. *Reviews of Modern Physics* 89, 1 (2017), 015002.
[6] Nana Georgiou and Victor Guillemin. 2015. Uncertainty Relations for Positive-Operator-Valued Measures. *Journal of Physics A: Mathematical and Theoretical* 48 (2015), 235203.
[7] Paul Hausladen and William K Wootters. 1994. A 'Pretty Good' Measurement for Distinguishing Quantum States. *Journal of Modern Optics* 41, 12 (1994), 2385–2390.
[8] Carl W Helstrom. 1976. Quantum Detection and Estimation Theory. (1976).
[9] Alexander S Holevo. 1973. Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. *Problemy Peredachi Informatsii* 9, 3 (1973), 3–11.
[10] Hans Maassen and Jos B M Uffink. 1988. Generalized Entropic Uncertainty Relations. *Physical Review Letters* 60, 12 (1988), 1103–1106.
[11] Tomohiro Ogawa and Hiroshi Nagaoka. 2007. Making Good Codes for Classical-Quantum Channel Coding via Quantum Hypothesis Testing. *IEEE Transactions on Information Theory* 53, 6 (2007), 2261–2266.

[12] Lev Stambler. 2026. Towards Simple and Useful One-Time Programs in the Quantum Random Oracle Model. *arXiv preprint arXiv:2601.13258* (2026). Section 6: Conclusion and Future Directions.
[13] Marco Tomamichel. 2012. A Framework for Non-Asymptotic Quantum Information Theory. *arXiv preprint arXiv:1203.2142* (2012).
[14] Stephen Wiesner. 1983. Conjugate Coding. *ACM SIGACT News* 15, 1 (1983), 78–88.
[15] Mark M Wilde. 2013. Quantum Information Theory. (2013).
[16] Andreas Winter. 1999. Coding Theorem and Strong Converse for Quantum Channels. *IEEE Transactions on Information Theory* 45, 7 (1999), 2481–2485.