RUHR-UNIVERSITÄT BOCHUM

Super-Quadratic Quantum Speed-Ups and Guessing Many Likely Keys

Timo Glaser, Alexander May, **Julian Nowakowski**

Main Result

Grover search + known probability distribution $\Longrightarrow$ super-quadratic speed-up

Key-Guessing Problem

Let k be a cryptographic key sampled from a distribution $\mathcal{D}$.

Given: oracle access to

$$f_k(x) := \begin{cases} 1, & \text{if } x = k, \\ 0, & \text{else.} \end{cases}$$

Find: k.

Optimal Algorithms

Classically:

- Enumerate keys in non-increasing order of likelihood.
- Expected runtime:

$$T_C(\mathcal{D}) = \sum_i i \cdot p_i,$$

with p_i the probability of the i-th most likely key.

Quantumly:

- Sophisticated variant of Grover search. Montanaro (TQC'11)
- Expected runtime:

$$T_Q(\mathcal{D}) = \sum_i \sqrt{i} \cdot p_i.$$

Known results

For the **quantum speed-up**

$$S(\mathcal{D}) := \frac{\log(T_C(\mathcal{D}))}{\log(T_Q(\mathcal{D}))},$$

the following is known:

- $S(\mathcal{D}) \geq 2$, for every $\mathcal{D}$.
- There exists $\mathcal{D}$ that makes $S(\mathcal{D})$ arbitrarily large.

Ambainis, de Wolf (STACS'00), Montanaro (TQC'11)

Impact for cryptographically relevant distributions unclear.

Arikan's Inequality (IEEE Trans. Inf. Theory, 1996)

For every $\rho \geq 0$,

$$\sum_i i^\rho \cdot p_i \approx 2^{\rho \, \mathrm{H}_{1/(1+\rho)}(\mathcal{D})},$$

where $\mathrm{H}_\alpha(\mathcal{D})$ denotes **Rényi Entropy** of order α.

Result so far missed in the cryptographic community.

Rényi Entropy

- $\mathcal{D}$ uniform $\Longrightarrow$ $\mathrm{H}_\alpha(\mathcal{D}) = \mathrm{H}_\beta(\mathcal{D})$ for all $\alpha, \beta \in [0, +\infty]$.
- $\mathcal{D}$ non-uniform $\Longrightarrow$ $\mathrm{H}_\alpha(\mathcal{D})$ decreases as α increases.

New Result

Arikan's inequality immediately yields

$$T_C(\mathcal{D}) \approx 2^{\mathrm{H}_{1/2}(\mathcal{D})}, \quad \text{and} \quad T_Q(\mathcal{D}) \approx 2^{\mathrm{H}_{2/3}(\mathcal{D})/2}.$$

In particular,

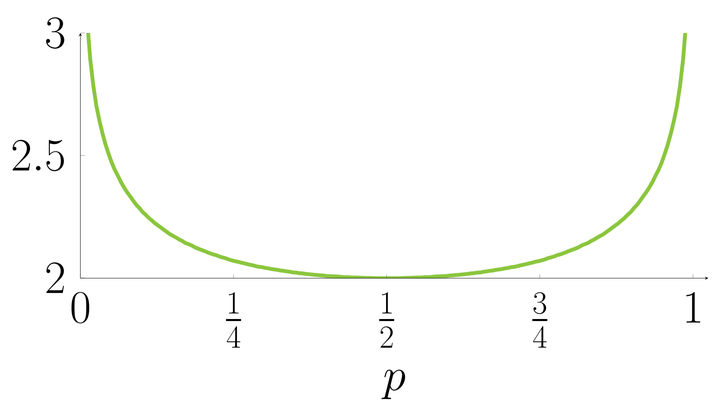
$$S(\mathcal{D}) \approx 2 \cdot \frac{\mathrm{H}_{1/2}(\mathcal{D})}{\mathrm{H}_{2/3}(\mathcal{D})} > 2.$$

($\mathcal{D}$ non-uniform)

Implications

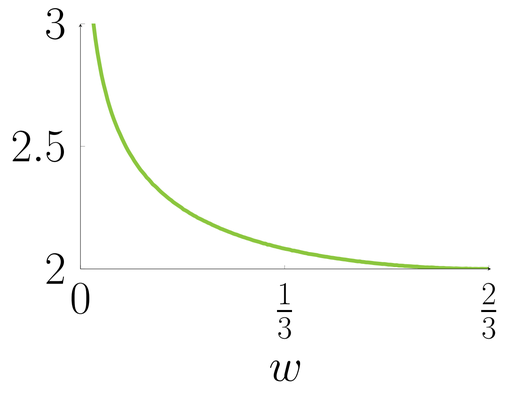
Bernoulli Distribution:

$\Pr[X = 0] = p$, $\Pr[X = 1] = 1 - p$, for $p \in (0, 1)$.



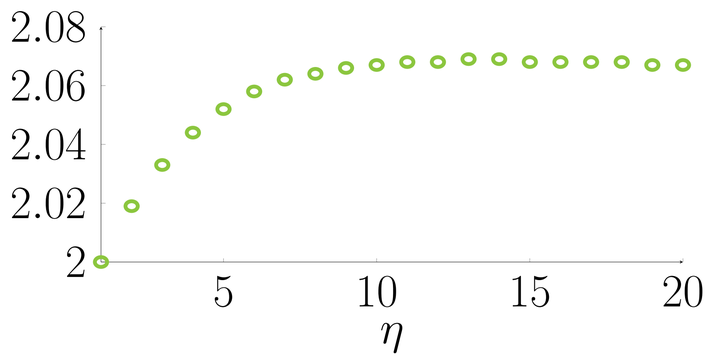
Weighted Ternary Distribution:

$\Pr[X = 0] = 1 - w$, $\Pr[X = 1] = \frac{w}{2}$, $\Pr[X = -1] = \frac{w}{2}$, for $w \in (0, \frac{2}{3}]$.



Centered Binomial Distribution:

$\Pr[X = i] = \binom{2\eta}{\eta+i} 2^{-2\eta}$, for $\eta \in \mathbb{N}$.



Additional Results in the Paper

We prove that guessing **some out of many** keys costs time

- $2^{\mathrm{H}_1(D)}$ classically, and
- $2^{\mathrm{H}_1(D)/2}$ quantumly.