# Quantum Computers Cannot Automate Theorem Proving
## (Unless Post-Quantum Cryptography Breaks)

**Noel Arteche**[1,2] Gaia Carenini[3,4] Matthew Gray[5]

[1]Lund University [2]University of Copenhagen [3]École Normale Supérieure (ENS) [4]University of Cambridge [5]University of Oxford

Poster based on *Quantum Automating* $\mathbf{TC}^0$*-Frege Is LWE-Hard*, which appeared at the Computational Complexity Conference (CCC 2024).

## Context

Given a true theorem, is there an efficient algorithm finding a proof for it? If not, what is the **computational complexity** of this task? In classical work form the 90s, Krajíček and Pudlák (1998) and Bonet, Pitassi, and Raz (2000) ruled out efficient proof search search unless a lot of classical cryptography, like RSA, breaks.

## Problem

This line of work **did not rule out the possibility of efficient quantum algorithms** for automating mathematics. Quantum computers breaks RSA due to Shor's algorithm, and many other cryptographic assumptions used in the 90s. **Could there be efficient quantum algorithms for proving mathematical statements?**

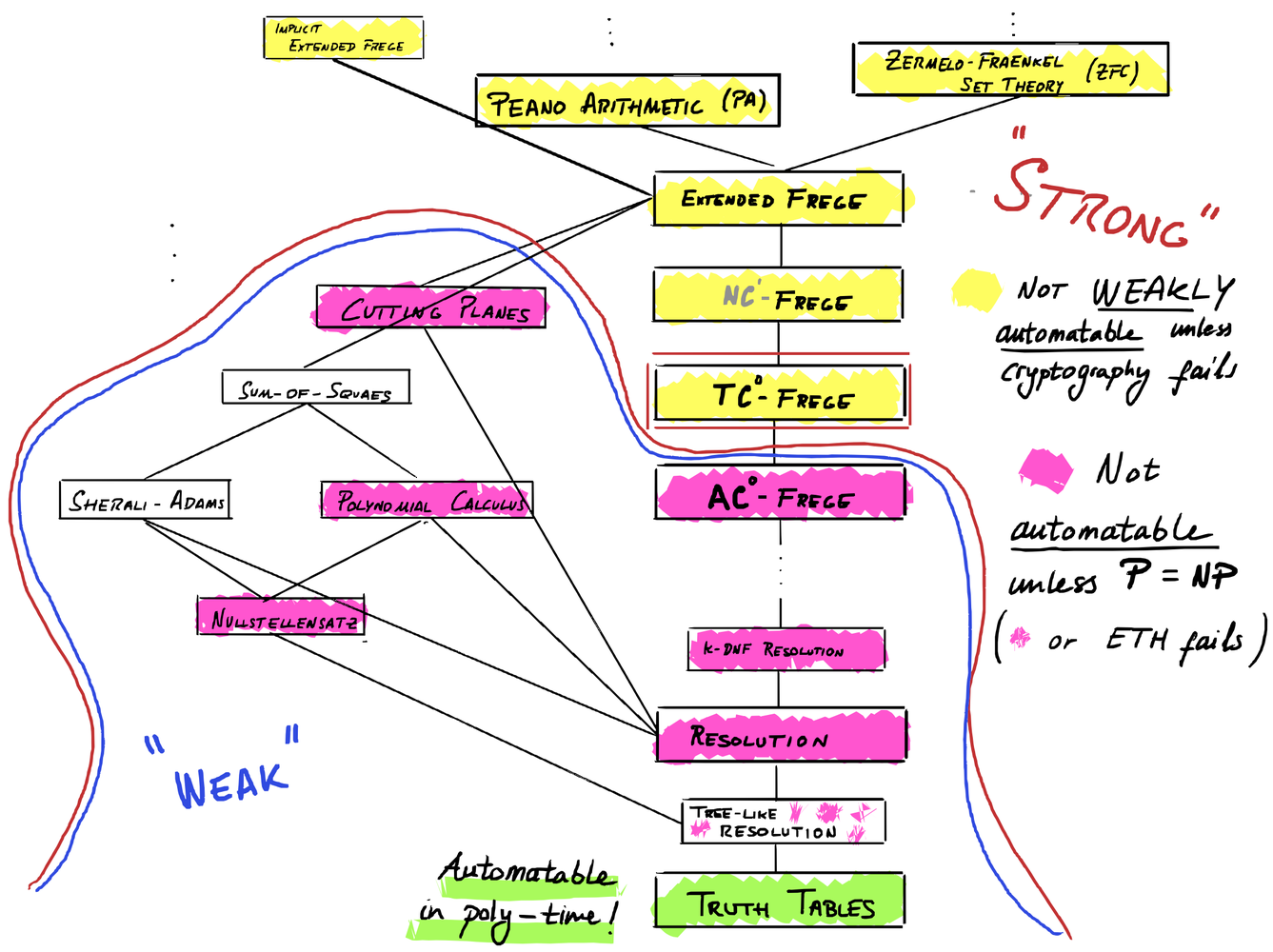
## Contribution

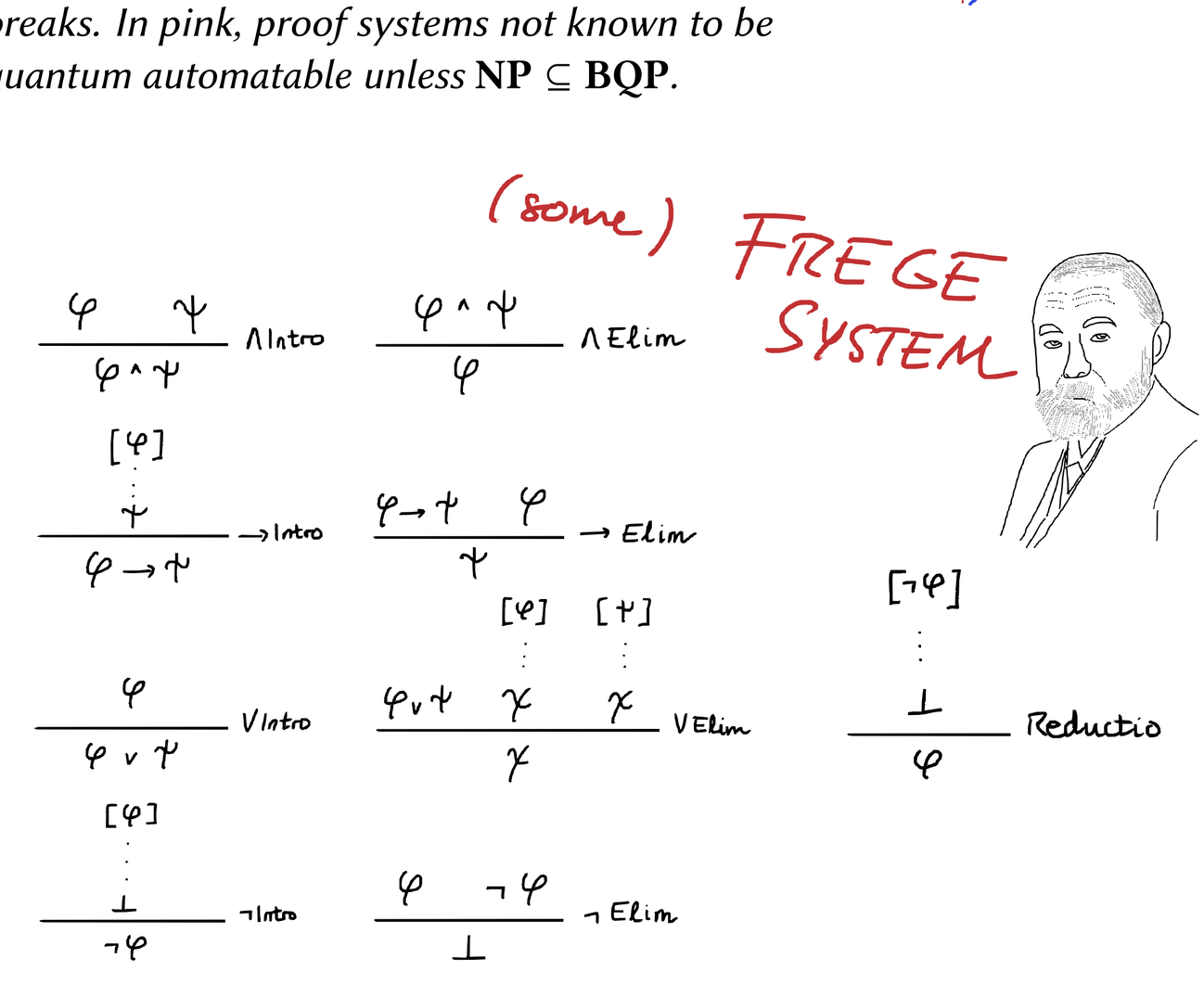
We prove that, if there exists an efficient quantum algorithm for finding proofs in any strong enough propositional proof system, then a lot of **post-quantum cryptography** believed to be secure will break! In particular, all the lattice-base cryptography based on the Learning with Errors (LWE) assumptions fails!

## Automating algorithms

The standard way to mathematically approach the study to proof search is via the framework of **automatability** pioneered by Bonet, Pitassi, and Raz (2000). For a given proof system $S$, an *automating algorithm*, if it exists, performs proof search in the following sense: given a statement $\varphi$ (encoded as a propositional tautology), outputs a proof $\pi$ in the system $S$ in time polynomial in the length of the shortest proof.

*On the right, different proof systems are arranged from weakest (at the bottom) to strongest (at the top). In yellow, proof systems known to be non-automatable unless LWE or Diffie-Hellman breaks. In pink, proof systems not known to be quantum automatable unless* $\mathbf{NP} \subseteq \mathbf{BQP}$.




## What kinds of proofs?

Our work applies to a large natural class of proof systems for propositional logic known as **Frege systems**. In particular, the result works for anything including $\mathbf{TC}^0$**-Frege**. Proof lines here lines are Boolean circuits from the class $\mathbf{TC}^0$, circuits with threshold gates and constant depth. These capture the power of contemporary neural networks! The system can efficiently reason about elementary combinatorics, linear algebra, and even analysis! We even showed that it can do some non-trivial lattice geometry.