1 Background

My undergrad studies in algebraic geometry provided me with a taste of categorial methods, mostly from the area of homological algebra but also with more basic constructions like (co-)limits, adjoint functors, natural transformations and sheaves. Although roughly familliar with the definition of a monoidal category I never worked with them in great detail. From my master studies in the area of cryptography I have knowledge of topics in complexity theory and quantum computation. Currently I am working on (tight) security proofs for cryptographic schemes against quantum adversaries and have undertaken simple research projects in this direction.

2 Order of Project Preferences

1. Simplifying quantum circuits using the ZX-calculus.

2. Complexity classes, computation, and Turing categories.

3-6. No Particular Order.

I am currently writing my masters thesis and will start my PhD shortly thereafter.

I can commit to coming to Oxford for both the conference and school.

CV

Personal Details

Name:	Maximilian Rath
Date of Birth:	02.01.1995
Adress:	Am Gosepötken 12 44795 Bochum
Telephone:	015787943664
E-Mail:	maximilian.rath@rub.de

Education

Since 2016	Study of Mathematics (M.Sc.) Ruhr-Universität Bochum Planned date of graduation: June 2019.
September 2013 - 2016	Study of Mathematics (B.Sc.) Universtität Bonn Minor in computer science. Bachelor Thesis: „The Motivic Zeta Function“ (1,3) Graduated in June 2016 with grade 1,7 („Good“)
2005-2013	Dietrich Bonhoeffer Gymnasium Metzingen. Graduated with „Abitur“ (1,5)

Language Skills

German (Native)

English (Proficient)

French (Beginner)

1 Research Statement

In the area of provably secure post quantum cryptography attackers are mostly modeled as (polynomially bounded) quantum algorithm. Thus it is of great interest to understand and model quantum algorithms. The ZX-calculus seems to be a promising (and so far the only) framework that works on a higher level than the basic quantum circuit model. With it, category theory has emerged as a nice organizing language and principle. (Even now, while mostly working in the Hilbert space formulation of quantum computation I find my thinking aided and greatly influenced by the few bits and pieces I glimpsed from the categorial formulation). Since these techniques are largely unexplored in the setting of post quantum cryptography, it would be interesting to see how they can be used to gain insight into things like

- Lower bounds on the quantum query complexity of certain problems.
- The various measures of distance of states and quantum channels, especially their relation and behaivour under standard transformations. Here quantitative results could directly translate to tight security reductions for cryptographic problems while qualitative results might still give insights into the general (in-)security of some cryptographic schemes.
- The construction and analysis of new quantum algorithms.

Moreover, building up contacts to researchers and graduate students from a field as young and diverse as applied category theory might yield interesting research problems and opportunities for future collaboration.