Background in Category Theory

I have read McLane's "Categories for Working Mathematician", Milewski's "Category Theory for Programmers" and Fong and Spivak's "Seven Sketches in Compositionality". However, I have no practice in working with categories for real scientific problems. I am working in the field of quantum informatics and our institute traditionally focuses in theoretical computer science.

PhD Thesis

Title: «Quantum information transmission. Effective cryptographic protocols»

Summary: Quantum hash functions allow to test that transmitted message was not altered; my thesis is devoted to generalizations.of quantum hash functions and their security.

I expect to defend my thesis in Spring 2019.

Order of Project Preference

1. Miriam Backens. Simplifying quantum circuits using the ZX-calculus
2. Pieter Hofstra. Complexity classes, computation, and Turing categories
3. Bartosz Milewski. Traversal optics and profunctors

Coming to Oxford

I can come to Oxford at my own expense if there would be some help with visa

Why I am interested in ACT 2019

I expect to get some experience with categories in real project at ACT and then use this experience in my area.

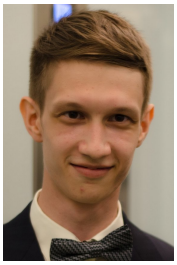
Quantum hashing maps a classical word to a quantum image, such that two different words have almost orthogonal images. It allows to map a word of length n to $O(\log \log n)$ qubits. Quantum hash functions are based on different objects: error-correcting codes (Burhman, Cleve, Watrous, de Wolf, 2003), small-biased sets (Vasiliev 2016), expander graphs, extractors (Ziatdinov 2016) etc. Properties of quantum hash functions can be proved using Chernoff-type bounds, but these proofs are a bit different. I believe that using categories in quantum hashing could allow generalizing them and highlight common structure in different quantum hash functions.

Other application of category theory lies in quantum cryptography. There are several proposed attacks on classical cryptosystems that are more efficient when performed on quantum computer than on classical. For example, there is an attack against iterated block ciphers by Kaplan (2014) that uses Ambainis algorithm and a slide attack that uses Simon's algorithm by Kaplan, Leurent, Leverrier and Naya-Plasencia (2016) that is exponentially faster that classical one. I believe that it is possible to define a general model of attacks that are performed on quantum computer (like the model of Wagner (2004) for classical block ciphers).

Mansur Ziatdinov

Curriculum Vitæ

ul. Zajni Sultana, d. 8, kv. 19
420073 Kazan
Russia
+7 (927) 670-72-60
http://kpfu.ru/Mansur.Ziyatdinov



To participate in Applied Category Theory 2019

Education

2005–2010 **Specialist (equivalent to MSc)**, *Kazan Federal university*, Kazan.

Specialist Thesis

Title Computational Power of Alternating Branching Programs [in Russian]

Supervisor Prof. F.M. Ablayev

Research Interests

- Quantum Cryptography
- Functional Programming

Experience

Occupation

2010– **Teaching Assistant**, *Kazan Federal University*.
Teached courses: Programming (Pascal, C++), Functional Programming, Cryptography, Network Security

Summer Schools

2015 **Summer School on Lower Bounds**, *Charles University*, Prague, Czech Republic.

2016 **Special Semester Program on Complexity Theory**, *St.Petersburg State University*.

Publications and Talks

Publications

F. Ablayev, M. Ablayev, A. Vasiliev, and M. Ziatdinov. Quantum Fingerprinting and Quantum Hashing. Computational and Cryptographical Aspects. *Baltic J. Modern Computing*, 4(4):860–875, 2016.

F. Ablayev, D. Bulychkov, D. Sapaev, A. Vasiliev, and M. Ziatdinov. Quantum-Assisted Blockchain. *Lobachevskii Journal of Mathematics*, 39(7):957–960, 2018.

A. Vasiliev, M. Latypov, and M. Ziatdinov. Minimizing collisions for quantum hashing. *Journal of Engineering and Applied Sciences*, 12(4):877–880, 2017.

M. Ziatdinov. Using frequency analysis and Grover's algorithm to implement known ciphertext attack on symmetric ciphers. *Lobachevskii Journal of Mathematics*, 34(4):313–315, 2013.

M. Ziatdinov. From graphs to keyed quantum hash functions. *Lobachevskii Journal of Mathematics*, 37(6):705–712, 2016.

M. Ziatdinov. Quantum Hashing. Group approach. *Lobachevskii Journal of Mathematics*, 37(2):222–226, 2016.

M. Ziatdinov. Attacking Quantum Hashing. Protocols and Their Cryptanalysis. *Lobachevskii Journal of Mathematics*, 39(7):1039–1045, 2018.

Conference Talks and Posters

F. Ablayev, M. Ablayev, A. Vasiliev, and M. Ziatdinov. Quantum Fingerprinting and Quantum Hashing: Cryptographical and Computational Aspects [in Russian]. In *Problems in Theoretical Cybernetics*, 2017.

A. Marchenko and M. Ziatdinov. Free Bi-Arrows, or How to generate programming course's assignments. In *Programming Languages and Compilers*. South Federal University, Rostov-on-Don, 2017.

A. Vasiliev and M. Ziatdinov. Minimizing Collisions of Quantum Hashing. In *Discrete Models in Controlling Systems Theory (in Russian)*, 2015.

M. Ziatdinov. On one technique of quantum hashing [in Russian]. In *Problems in Theoretical Cybernetics*, 2014.

M. Ziatdinov. On some types of composition of quantum hash generators [in Russian]. In *Problems in Theoretical Cybernetics*, 2014.

M. Ziatdinov. Quantum hashing based on symmetric groups. In *Current Trends in Cryptology*, Kazan, 2015.

M. Ziatdinov. Authenticating messages using quantum MAC based on graphs. In *Problems in Theoretical Cybernetics*, 2017.

M. Ziatdinov. Quantum Hashing and Quantum MAC. In *Quantum Fingerprinting and Quantum Walks*. Latvia University, 2017.

M. Ziatdinov. The Security of the Quantum MAC. In *3rd International Conference for Young Quantum Information Scientists*. Friedrich-Alexander Universität Erlangen-Nürnberg, 2017.

M. Ziatdinov. Attacking Quantum Hashing. Protocols and their Cryptanalysis. In *SOFSEM 2018 - 44th International Conference on Current Trends in Theory and Practice of Computer Science - Student Research Forum*. Danube University Krems, Austria, 2018.

Computer Skills

Programming languages	C, C++, **Haskell**, **Clojure**, Java, Pascal, Common Lisp
Markup, Scripting	**LaTeX**, HTML, CSS, JS, bash, regular expressions
Environment	**Git**, Mercurial, Make, Wiki/Markdown
Operating systems	**GNU/Linux**, Windows

Programming Projects

Github	`https://github.com/gltronred`
Bitbucket	`https://bitbucket.org/gltronred`