About

Gorjan Alagic
Associate Research Scientist
Joint Center for Quantum Information and Computer Science (QuICS)
University of Maryland

e-mail: galagic@gmail.com
tel: +1 301 250 5851
www: www.alagic.org
citizenship: USA

Research

Quantum computation, Cryptography

Education

University of Connecticut, Storrs, CT, USA
Advisor: Alexander Russell
Ph.D., Mathematics (2008): *Uncertainty Principles on Compact Groups*
M.S. (2005) and B.S. (2003) in Mathematics

Positions

University of Maryland, College Park, MD, USA
Associate Research Scientist, UMIACS **2019 -**
Adjunct Fellow, QuICS **2017 -**
Assistant Research Professor, UMIACS **2017 - 2019**

NIST, Gaithersburg, MD, USA **2017 -**
Guest Researcher, Computer Security Division

University of Copenhagen, Copenhagen, DK **2014 - 2017**
Postdoctoral Scholar, QMATH, Department of Mathematical Sciences

Caltech, Pasadena, CA, USA **2011 - 2014**
Postdoctoral Scholar, Institute for Quantum Information and Matter

University of Waterloo, Waterloo, ON, Canada **2008 - 2011**
Postdoctoral Fellow, Institute for Quantum Computing

University of Connecticut, Storrs, CT, USA **2003 - 2008**
Research/Teaching Assistant, Dept. of C.S.E. & Dept. of Mathematics

Grants

Practical Quantum Protocols **2020 - 2023**
Air Force Office of Scientific Research; $795,000;
Principal Investigator. Gorjan's portion: $265,000.

Quantum algorithms for algebra and discrete optimization **2020 - 2023**
US Army Research Office; $745,000;
Principal Investigator. Gorjan's portion: $150,000.

Fundamental Algorithmic Research for Quantum Computing **2020 - 2025**
US Department of Energy; Large-scale, multi-institution, $20 million total;
co-PI. Gorjan's portion: $400,000.

AF Medium: Collaborative: Quantum-Secure Cryptography **2018 - 2021**
National Science Foundation; Multi-institution, $825,000 total;
Principal Investigator for UMD. Gorjan's portion: $275,000.

TQC + NISQ (2019) conference support (with Aarthi Sundaram) **2019**
National Science Foundation; $10,000 student travel support (PI);
Air Force Office of Scientific Research; $15,000 conference support (PI);
Department of Energy; $20,000 conference support (PI);

Publications

Efficient simulation of random states and random unitaries
(with C. Majenz and A. Russell),
Proceedings of EUROCRYPT'20.

Quantum-secure authentication via blind-unforgeability
(with C. Majenz, A. Russell, F. Song),
Proceedings of EUROCRYPT'20; presented at QCrypt '18.

On quantum chosen-ciphertext attacks and Learning with Errors
(with S. Jeffery, M. Ozols, and A. Poremba),
Proceedings of TQC'19; presented at QCrypt '18.

Unforgeable quantum encryption
(with T. Gagliardoni and C. Majenz),
Proceedings of EUROCRYPT'18; presented at QCrypt '18.

Spectrum estimation of density operators with alkaline-earth atoms
(with M. Beverland, J. Haah, G. Campbell, A. Rey, A. Gorshkov),
Phys. Rev. Lett. 120, 025301 (2018); presented at QIP'16.

Quantum fully-homomorphic encryption with verification
(with Y. Dulek, C. Schaffner, F. Speelman),
Proceedings of ASIACRYPT'17; presented at QCrypt'17, QIP'18.

Quantum non-malleability and authentication
(with C. Majenz), *Proceedings of CRYPTO'17*; presented at QCrypt'17, AQIS'17.

Quantum-secure symmetric-key cryptography based on hidden shifts
(with A. Russell), *Proceedings of EUROCRYPT'17*; presented at TQC'17.

3-manifold diagrams and NP vs #P
(with C. Lo), *Quantum Info. and Computation*, 17(1&2): 125-141 (2017).

Computational security of quantum encryption
(with A. Broadbent, B. Fefferman, T. Gagliardoni, C. Schaffner, M. St Jules),
Proceedings of ICITS'16; presented at QCrypt'16.

Realizing exactly solvable SU(N) magnets with thermal atoms
(with M. Beverland, M. Martin, A. Koller, A. Rey, A. Gorshkov),
Physical Review A 93 (5), 051601 (2016).

Yang-Baxter operators need quantum entanglement to distinguish knots
(with M. Jarrett and S. Jordan), *Journal of Physics A*, 49 075203 (2016).

Classical simulation of Yang-Baxter gates
(with A. Bapat and S. Jordan), *Proceedings of TQC'14*.

Circuit obfuscation using braids
(with S. Jeffery and S. Jordan), *Proceedings of TQC'14*.

Collaborative Mathematics learning in online environments

(with M. Alagic), *Visual Mathematics and Cyberlearning*, Vol. 1 in series on Mathematics Education in the Digital Era; Springer-Verlag (2013).

Quantum algorithms for invariants of triangulated manifolds
(with E. Bering), *Quantum Info. and Computation* 12(7&8):843-863 (2012).

Turaev-Viro invariant of mapping tori is complete for one clean qubit
(with S. Jordan) *Proceedings of TQC'11*.

Spectral concentration of positive functions on compact groups
(with A. Russell), *Journal of Fourier Analysis and Appl.* 17(3):355-373 (2011).

Turaev-Viro 3-manifold invariant is universal for quantum computation
(with S. Jordan, R. König, B. Reichardt), *Physical Review A* 82, 040302(R) (2010).

Quantum algorithms for Simon's problem over general groups
(with C. Moore and A. Russell), *ACM Trans. on Algorithms* 6(1) (2009); *Proceedings of SODA'07*.

Uncertainty principles for compact groups
(with A. Russell), *Illinois Journal of Mathematics* 52(4):1315-1324 (2008).

Quantum computing and the hunt for hidden symmetry
(with A. Russell), *Bulletin of the European Association for Theoretical Computer Science* 93:53-75 (2007).

Decoherence in quantum walks on the hypercube
(with A. Russell), *Physical Review A* 72, 062304 (2005).

Unpublished works

Impossibility of Quantum VBB Obfuscation of Classical Circuits
(with Z. Brakerski, Y. Dulek and C. Schaffner), preprint.

Non-interactive classical verification of quantum computation
(with A. Grilo, S. Hung and A. Childs), preprint.

On quantum obfuscation
(with B. Fefferman), presented at QCrypt '16.

Can you sign a quantum state?
(with T. Gagliardoni and C. Majenz), to be presented at QCrypt '19.

Students

Chen Bai: *Cryptography in the presence of quantum queries* (2019 -);
PhD student, ECE, University of Maryland.

Bibhusa Rawal: *Quantum security of Even-Mansour cipher* (2018 -);
PhD student, ECE, University of Maryland.

Alexander Poremba: *Learning with Errors from quantum samples* (2017);
MSc Physics, U. Heidelberg; now PhD student at Caltech.

Hector Hougaard: *Pseudorandom permutations on groups* (2017);
MSc Mathematics, U. Copenhagen; now PhD student at Osaka University.

Erik Partridge: *Time-reversible quantum programming languages* (2016);
MSc Computer Science, U. Copenhagen; now working in industry.

Catharine Lo: *Complexity theory and 3-manifold invariants* (2014);
Caltech SURF fellow; now PhD student in Mathematics at Princeton.

Evan Patterson: *Quantum algorithms, Fourier analysis on compact groups* (2013);
Caltech SURF fellow; now PhD student in Statistics at Stanford.

Aniruddha Bapat: *Classical simulation of Yang-Baxter gates* (2012);
Caltech SURF fellow; now PhD student in Physics at Univ. of Maryland.

Edgar Bering: *Quantum algorithms for manifold invariants* (2010);
U. of Waterloo REU fellow; now a postdoc at Temple University.

SERVICE

Teaching. All courses taught as main instructor.

- University of Maryland (2020 -):
  - Spring 2020 : *CMSC 456: Cryptography* (Symmetric and public-key encryption, message integrity, hash functions, block-cipher design and analysis, number theory, digital signatures, etc.).
- University of Copenhagen (2015 - 2017):
  - *Introduction to Modern Cryptography* (private-key and public-key cryptography, Diffie-Hellman, El-Gamal, DSA, Learning with Errors, FHE);
  - *Representation Theory* (finite and compact groups, Schur’s Lemma, Peter-Weyl theorem, Lie groups and Lie algebras, highest weight theory.)
- University of Connecticut (2003 - 2006):
  - *Elementary Mathematical Modeling*;
  - *Introductory Calculus*;
  - *Problem Solving*.

Organization.

- Masterclass on Quantum Mathematics, Copenhagen (2015). Workshop with invited speakers; 70 attendees. Local organizer (with Robin Reuvers.)
- TQC + NISQ (2019). Major 3-day conference and co-located 2-day workshop with contributed and invited talks, and poster and industry sessions; 250+ attendees. Local organizer (with Aarthi Sundaram.)

Conference committees; reviewing.

- Program Committee member: PKC ‘20; Asiacrypt ’19 and ‘20; PQCrypto ’18 and ’19; QCrypt ’17; TQC ’13 and ’16.
- Steering Committee member. TQC (’19 - present); QCrypt (‘19 - present).
- Reviewer. QIP, STOC, Eurocrypt, QIC, LATIN, SICOMP, RANDOM, Quantum, PRL, PRA, etc.

Editor. Academic editor, PLOS ONE (2018 - 2020)

Student representative. Senator, UConn Graduate Student Senate; Student Representative, Mathematics Graduate Faculty (2004 - 2005)

SELECTED TALKS

Can you sign a quantum state?
[invited] QCrypt ‘19, Montreal, CA (2019);

Classical functions unpredictable to quantum adversaries
[invited] Quantum Algorithms workshop, Microsoft Quantum (2018);

Quantum non-malleability and authentication
QCrypt ‘17, Cambridge, UK (2017);

Quantum-secure symmetric-key cryptography from Hidden Shifts
Quantum Cryptanalysis Workshop, Dagstuhl, Germany (2017);
TQC ‘17, Paris, France (2017);
EUROCRYPT ‘17, Paris, France (2017);

Superposition attacks and fully-quantum crypto

U.S. National Institute of Standards and Technology, MD (2017);
QuICS center, University of Maryland (2017);

Internet cryptography for quantum data
QMATH Kick-off conference, University of Copenhagen (2016);
Microsoft Research, Redmond, WA (2016);

How to encrypt a quantum state
QuiCS Seminar, University of Maryland (2016);

Hidden shifts and quantum attacks on symmetric-key cryptography
U.S. National Institute of Standards and Technology, MD (2016);

Provable Security and Quantum Encryption
[invited] Winter School on Quantum Security, Darmstadt (2016);

Quantum encryption and obfuscation
Workshop on quantum computation, Aspen (2016);
Workshop on quantum cryptanalysis, Dagstuhl (2015).

On the impossibility of quantum obfuscation
IQIM Seminar, Caltech, Pasadena (2016);
[invited] Workshop on quantum info. and crypto., Aarhus (2015).

Two results in topology, motivated by quantum computation
[invited] American Physical Society March meeting, San Antonio (2015);
IQIM Seminar, Caltech, Pasadena (2015).

Classical simulation of Yang-Baxter gates
Theory of Quantum Comp., Comm., Crypto. (TQC), Singapore (2014).

Candidate classical and quantum circuit obfuscation
U.S. National Institute of Standards and Technology, MD (2014).

Harmonic analysis and Marcinkiewicz-Zygmund inequalities
IQI meeting, Caltech (2014).

Quantum computation and mapping class groups
[invited] Colloq. on Group-Theoretical Methods in Physics, Tianjin (2012).

Circuit obfuscation with braids
IQIM Seminar, Caltech, Pasadena (2012).

Quantum computation and low-dimensional topology
Wichita State University (2011).

Turaev-Viro invariant of mapping tori is DQC1-complete
Theory of Quantum Comp., Comm., Crypto. (TQC), Madrid (2011).

Approximating Turaev-Viro 3-manifold invariants is BQP-complete
Asian Conf. on Quantum Information Science (AQIS), Tokyo (2010).

Quantum algorithms from topological quantum field theories
Workshop on Quantum Algorithms and Foundations, Vancouver (2010).

Quantum computation with topological lattice field theories
Perimeter Institute, Waterloo (2009).

Quantum algorithms for product groups
Institute for Quantum Computing, University of Waterloo (2008);
Los Alamos National Laboratories (2008).

Quantum algorithms for Simon's problem over general groups
ACM-SIAM Symposium on Discrete Algorithms, New Orleans (2007).

Uncertainty principles on finite groups
New York Number Theory Seminar, City University of New York (2006).

Decoherence in quantum walks on the hypercube
NES MAA Fall 2005 Meeting, University of New Hampshire (2005).