**2nd QSC General Assembly (Friday June 21)**

**Date and Time**

Friday, June 21, 2019. The technical program starts as 10:45h (walk-in as of 10:15h).

**Location**

Zuidas Business & Conference Center, WTC (“World Trade Center”)

Strawinskylaan 77, 1077 XW Amsterdam

This is right next to the Amsterdam Zuid train and metro station.

**Program**

10:15 - 10:45     WALK-IN

10:45 - 11:30     Shelby Kimmel (Middlebury College):

*Path detection: A quantum algorithmic primitive*

11:30 - 12:15     Sebastian de Bone (QuTech):

*Creation and purification of GHZ states from EPR pair configurations*

12:15 - 13:30     LUNCH

13:30 - 13:45     Harry Buhrman (QuSoft & CWI & UvA):

*QSC State-of-the-Union - Report on progress*

13:45 - 14:30     Ronald de Wolf (QuSoft & CWI & UvA):

*The potential impact of quantum computers on society*

14:30 - 15:15     Peter Bruin (UL):

*On quantum computation of Kloosterman sums*

15:15 - 15:45     BREAK

15:45 - 16:30     Benjamin Wesolowski (CWI):

*Quantum algorithms for finding short vectors in ideal lattices*

16:30 - 17:15     David DiVincenzo (Jülich Research Center & Aachen University & TU Delft):

*Constructing the quantum computer -- the role of model building*

17:15         RECEPTION

**Registration**

Registration is **free but required.**

Please register by sending an email to Susanne van Dam ([Susanne.van.Dam@cwi.nl](mailto:Susanne.van.Dam@cwi.nl)) with the subject “QSC-GA Registration”, stating your name and affiliation. You may also mention dietary restrictions and add further comments (e.g. if you skip lunch or the reception).

**Speakers and Abstracts**

**Sebastian de Bone** (QuTech)

*Title*: Creation and purification of GHZ states from EPR pair configurations

*Abstract*: This presentation discusses theoretical work on protocols that create and purify GHZ states out of EPR pairs shared between the involved network parties. GHZ states have many applications in quantum information and the upcoming quantum internet. They also play an important role in error correcting architectures for distributed quantum computation, which investigates the possibilities of using EPR pairs to create an entangled network of quantum computers. By using the stabilizer formalism, we are able to place GHZ creation protocols in a common framework. This allows us to propose new protocols that, compared to existing protocols, perform better in particular situations of interest.

*Bio*: Sebastian de Bone is a PhD student at TU Delft and CWI, working on scalable architectures for distributed quantum computation. He is supervised by Dr. David Elkouss Coronas (TU Delft / QuTech) and Dr. Stacey Jeffery (CWI / QuSoft). Sebastian graduated in Applied Physics at the University of Twente.

**Peter Bruin** (UL)

*Title*: On quantum computation of Kloosterman sums

*Abstract*: Kloosterman sums are an important kind of complex-valued "special functions" on finite fields.  They are analogous to Bessel functions and occur in Fourier analysis on Euclidean spaces (over finite fields in this case) in the presence of rotational symmetries.  I will speak about quantum algorithms to compute Kloosterman sums, with an application to the hidden radius problem, where the goal is to find the radius of a family of translates of a sphere in a Euclidean space over a finite field that is hidden by a black-box function.

*Bio*: Peter Bruin obtained his PhD in Leiden in 2010. Subsequently, he worked as a postdoc at the Université Paris-Sud and the Universität Zürich, and as a lecturer at the University of Warwick. He has been an assistant professor in Leiden since 2014. He has worked on various topics in number theory and arithmetic geometry, with algorithmic and explicit methods as a common theme. Most recently, he has become affiliated with the Quantum Software Consortium and has been working on building bridges between number theory and quantum computing.

**David DiVincenzo**  (Jülich Research Center & Aachen University & TU Delft)

*Title*: Constructing the quantum computer -- the role of model building

*Abstract*: A present view of a solid state quantum computer is that a major part of it is a large assembly of extremely low loss electrical structures, of varying degrees of anharmonicity (large anharmonicity=qubit), coupled into a two dimensional network. I will review some approaches that we have laid out for simulating these structures to determine reliable parameters for quantum (Hamiltonian) modeling. We see that current approaches may not be modular (=scalable) enough. I mention some new design schemes that we are working on to circumvent this.

Bio: David DiVincenzo (Philadelphia, VS, 1959) is Director, Theoretical Nanoelectronics, Forschungszentrum Jülich (Germany). He received his doctorate at the University of Pennsylvania, Philadelphia, USA in 1983; was a postdoc at Cornell University, Ithaca, USA; then Research Staff Member at IBM Watson Research Center, Yorktown Heights, New York, USA (1985-2011). Having been granted an Alexander von Humboldt Professorship in 2010, he became a professor at the Institute of Theoretical Quantum Information at RWTH Aachen University and director of the Peter Grünberg Institute, where he serves to the present. He is a Fellow of the American Physical Society (1999), and Associate Editor of the Reviews of Modern Physics (2011-present). DiVincenzo was one of the first physicists to engage in quantum information research and is considered an authority on quantum information processing. In particular, his name is associated with the development of criteria for the quantum computer, known as the DiVincenzo Criteria, and also with the Loss-DiVincenzo approach to solid-state spin-based qubits.

**Shelby Kimmel** (Middlebury College)

*Title*: Path detection: A quantum algorithmic primitive

*Abstract*: "st-connectivity" is the problem of deciding whether two points in a graph are connected or not (i.e. whether there is a path between them). I will show that a range of common problems can be reduced to st-connectivity, and furthermore, this reduction leads to an optimal quantum algorithm in many cases of interest. The analysis of the quantum algorithm is fairly simple, and uses standard graph theoretic quantities. These properties suggest that st-connectivity would make a good building block, or primitive, for designing and analyzing quantum algorithms.

*Bio*: Shelby Kimmel is an Assistant Professor of Computer Science at Middlebury College where she enjoy working with undergraduates in the classroom and on research. Previously, she was a Hartree Postdoctoral Fellow at the University of Maryland in QuICS - the Joint Center for Quantum Information and Computer Science. She earned a PhD in physics from MIT and a BA in astrophysics from Williams College.

**Benjamin Wesolowski** (CWI)

*Title*: Quantum algorithms for finding short vectors in ideal lattices

*Abstract*: The security of a number of post-quantum cryptographic schemes relies on the presumed hardness of computational problems over structured lattices. Finding short vectors in so-called ideal lattices has long been assumed to be hard, even with the help of a quantum computer. However, in recent years, a series of results have challenged this assumption: new algorithms allow to find unexpectedly short vectors in cyclotomic ideal lattices in quantum polynomial time, under some heuristic assumptions. We will present the current state of affairs, and the relevance of these quantum algorithms for the standardisation of lattice-based cryptography. This is based on joint works with Ronald Cramer, Léo Ducas and Maxime Plançon.

*Bio*: Benjamin Wesolowski obtained his PhD in 2018 from the Ecole Polytechnique Fédérale de Lausanne (EPFL). His research focuses on arithmetic and geometric structures used in cryptography, notably related to the discrete logarithm problem, the structure of isogeny graphs, and the geometry of structured lattices. Since 2019 he is a postdoctoral researcher at the Cryptology group of CWI.

**Ronald de Wolf** (QuSoft, CWI and University of Amsterdam)

*Title*: The potential impact of quantum computers on society

*Abstract*: This talk considers the potential impact that the nascent technology of quantum computing may have on society. It focuses on three areas: cryptography, optimization, and simulation of quantum systems. We will also discuss some ethical aspects of these developments, and ways to mitigate the risks.

*Bio*: Ronald de Wolf (1973) studied computer science and philosophy at the Erasmus University Rotterdam, with a focus on logic-based machine learning. He obtained his PhD in 2001 from the University of Amsterdam and CWI (advised by Harry Buhrman and Paul Vitanyi) on a thesis about quantum computation and communication complexity, for which he received the 2003 ERCIM Cor Baayen Award. Subsequently he worked as a postdoctoral researcher at UC Berkeley. Currently he is a senior researcher at CWI and full professor at the University of Amsterdam. He works on quantum computing, focusing on algorithms, complexity theory, and the applications of quantum information to other areas.

**Organizers**

Scientific organizers: Ronald Cramer (CWI & UL), Bas Edixhoven (UL), Serge Fehr (CWI & UL)

Secretary: Susanne van Dam