Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-16-44

How to Apply **Create and release your Profile on Zintellect** – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 2 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Application Deadline 4/15/2016 6:00:00 PM Eastern Time Zone

Description Quantum computation is a novel computing paradigm which goes beyond what existing computers are capable of. In particular, problems such as the factorisation of large numbers, which are currently thought to be hard to solve on conventional computers, are easy to solve on quantum computers. Since much of modern cryptography depends on the difficulty of solving such problems, the advent of a practical quantum computer of any size would have a devastating effect on the security of existing communication systems.

The theory of quantum computation and its effect on cryptography has been known for some time and there has been considerable research effort on building practical quantum computers. This research has reached the point where it is reasonable to assume that practical quantum devices will be available in the medium term – and at the very least it is necessary to take steps to guard against the risk that such devices would pose to communication security.

Post-quantum cryptography refers to the use of (classical) cryptography secure against the likely capabilities of a quantum computation likely to be developed in the medium term. It is known that conventional public-key cryptography, on which internet security largely depends, is vulnerable to Shor's algorithm running on a quantum computer. Research into the development, costing, assessment and implementation of new forms of cryptography is needed.

(It should be noted that quantum communication – using quantum effects to establish secure communication channels – is not part of this topic)

Example Approaches:

A number of approaches such as lattice-based cryptosystems and learning-with-errors hav been proposed and studied in the open literature and in the intelligence community. Some have been shown to be vulnerable to new quantum algorithms, such as SOLILOQUY. The scope of this project might include either of the following:

- Assessment of the quantum complexity of breaking currently proposed cryptographic algorithms. The key part of this approach is not to accumulate new primitives as such, but to develop a capability for assessing their security in terms of quantum complexity. Alternatively development of new and practical primitives with “built-in” complexity proofs. This might involve research into the theory of quantum complexity and its relation to classical complexity.
- Development of quantum costing methodologies, to assess the costs of currently proposed or likely quantum computational systems in terms of time, energy and money. This could require collaboration with the groups currently researching quantum technology. This work could be aligned with current paradigms for recommendations for levels of security in classical cryptosystems as proposed, for example, by CESG.

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Business** (11 👁)
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (6 👁)
  - **Computer, Information, and Data Sciences** (16 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (10 👁)
  - **Other Non-Science & Engineering** (13 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (28 👁)