zintellect
climb higher

Opportunity Title: Full homomorphic encryption of data for low bandwidth channels
Opportunity Reference Code: IC-18-21

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-18-21

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.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orau.org/icpostdoc/.

If you have questions, send an email to ICPostdoc@orau.org.   Please include the reference code for this opportunity in your email.

Application Deadline 3/12/2018 11:59:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

- At a high level of abstraction, data in a network system is either in motion, at rest, or in use. Data in motion and at rest may be protected via digital encryption. However encrypted data, prior to use by a processor, are usually decrypted first at which point the data can be vulnerable to cyber-attack. Shielding and other protection methods may not provide enough defense if a malicious actor is able to approach in the vicinity of the processor.
- An emerging option is to never decrypt the data but instead use full homomorphic encryption (FHE). With FHE, the processor can perform computations on the encrypted bits without exposing the clear (decrypted) data for someone to see.
- Much of literature and recent papers suggest that homomorphic encryption is still not practical due to its heavy computational burden, but it might be worth exploring its use in low bandwidth channels.A generic system may, for example, have many embedded sub-systems, each with low bandwidth processes.
- The goal of this effort is to study and explore the potential use of recently emerged FHE developments (post 2011) for use with executable binaries, especially with the executing processor logic in software (e.g., written for FPGAs and GPUs).

Example Approaches:

- Full homomorphic encryption (FHE) of secure low bandwidth channels in low SWaP embedded devices (e.g., microcontrollers).

- Consider other cryptologic approaches.
- Application of novel methods to a particular use case (e.g., a control channel) with realized data, even if only simulated in the absence of real data.

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the application deadline
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program.

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **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** (5 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (28 👁)