International Summer Program/Internship in Applied MPC and Implementations

**Location:** Bar-Ilan University, Ramat Gan, Israel (Tel Aviv area)

**Dates:** June 3 – July 26, 2018 (note that the work week in Israel is Sunday – Thursday)

**Aim:** The aim of the program is for International and Israeli graduate students to learn about the applied aspects of secure multiparty computation, including implementation issues.

**Prerequisites:** Participating students must be in a graduate program and have taken a recognized course in cryptography. Basic familiarity with secure multiparty computation is required, and students with in-depth knowledge will be given preference. Students must have strong programming skills, including in-depth knowledge of C++.

All participants are expected to watch the lectures from the first 4 days of the 5th BIU winter school in MPC before the program starts (i.e., lectures on material that they are not familiar with). See [https://cyber.biu.ac.il/event/the-5th-biu-winter-school/](https://cyber.biu.ac.il/event/the-5th-biu-winter-school/). The TPMPC workshop ([http://www.multipartycomputation.com/tpmpc-2018](http://www.multipartycomputation.com/tpmpc-2018)) will take place in Denmark the week before the program begins; participation in the workshop will be beneficial.

**Program elements:**

1. The summer program includes a series of lectures on applied MPC, given by BIU and possibly other invited faculty.
2. The program includes a series of lectures on MPC implementation principles (libraries, networking, primitives, optimizations) by the software engineering group at BIU.
3. Students will receive MPC papers describing efficient protocols. The students will first study the papers that they received and present them to the rest of the group. Questions and challenges regarding efficiency and implementations will be discussed by the group. The students will then implement the protocol in the paper they have been given. Depending on the paper in question, some students will work in groups.
4. More advanced graduate students may receive papers that require research before implementation (e.g., choosing which instantiations of primitives are best; this is non-trivial for some protocols, like the MPC-in-the-head family of protocols).
5. Students will receive mentoring by the BIU software engineering group regarding implementation tips and techniques, and will learn strategies for efficient MPC implementations including how to use profilers to detect inefficiencies and improve them. Students will be expected to write high-quality code that will be incorporated into BIU’s open-source library of MPC implementation.
6. Depending on time, students will work to optimize and improve on the protocols, and demonstrate the improvements in running time.
Cost: The BIU center for research in applied cryptography and cyber security will cover the travel and lodging expenses of accepted participants. All participants will also receive a daily stipend of 100 NIS per day (5,600 for the entire 8-week period).

How to apply: Please send your CV and a letter of recommendation from your advisor to lindell@biu.ac.il. Please make sure to include all relevant background knowledge and expertise (including programming knowledge).

Application deadline: April 15, 2018