MEMORANDUM OF UNDERSTANDING
between
Tel Aviv University (TAU), Tel Aviv, Israel
and
Indian Institute of Technology Kanpur, Kanpur, India
MEMORANDUM OF UNDERSTANDING between Tel Aviv University (TAU), Tel Aviv, Israel and Indian Institute of Technology Kanpur, Kanpur, India

1. General
2. Cooperative research and teaching projects
   2.1 Personnel Exchange
   2.2 Joint workshops
   2.3 Visiting scholars’ seminars
   2.4 Facilitation of joint collaboration in long-term research
   2.5 Exchange of information, advice and best practices concerning the design of research laboratories and centers
   2.6 Exchange of scientific materials
3. Administration, logistics and budget
4. Representatives
5. Entire Agreement/Modification
6. Academic Freedom
7. Intellectual Property (IP)
8. Export Compliance
9. Indemnification
10. Conduct
11. Use of Name
12. Language of Execution
13. Term, Duration, Variation and Termination
14. Appendix I: Prospective topics for joint research
   14.1 Security by design of future complex cyber-physical systems, including IoT and the following subjects
   14.3 Comprehensive interdisciplinary cybersecurity: integrating political, social, economic, and human non-technical factors with the core science and engineering disciplines, such as
   14.4 Security of cyber-physical systems in priority sectors such as
   14.5 Concepts, methods and mechanisms for improving cybersecurity while upholding core social values, such as
   14.6 International cybersecurity and power, such as
   14.7 Cybersecurity as an essential instrument for knowledge-based economic development and inclusive growth, such as
1. General

The IITK and The TAU Blavatnik Interdisciplinary Cyber Research Center (ICRC) missions have a lot in common. Both strive to become an internationally renowned and nationally the most important center for research, education, public awareness, and national service for securing and defending their national critical infrastructures from cyber-attacks and electronic warfare, and the center to create next generation work force in cyber security. International cooperation in research and innovation actions is known to produce mutual benefits.

In order to better fulfil their respective missions, representatives from the two institutions have exchanged views on establishing relationships and a program of cooperation between the two institutions.

**Tel Aviv University** (hereinafter “TAU”) and the **Indian Institute of Technology Kanpur** (hereinafter “IITK”) agree to establish this Memorandum of Understanding (hereinafter “MOU”) as a framework for cooperation. This MOU is made and entered into by and between TAU and IITK establishing the basis for cooperation between the two institutions with the following provisions.

2. **Cooperative research and teaching projects**

To facilitate bi-lateral academic scientific relationships and to develop cooperative research and teaching projects in selected fields as mutually agreed upon by the two universities, **TAU ICRC** and **IITK Computer Science and Engineering Department** envision several types of activities (hereinafter “projects”). Six types of such projects are listed below.

2.1. **Research Projects**

Graduate student, postdoctoral researcher, and faculty exchanges will be performed on a regular basis to both host universities, to exchange knowledge, experience and ideas stimulating mutually beneficial research.

**Visiting Professors**

As resources permit, members of the faculty at one institution will be invited to serve as visiting members of the faculty of the other. Visiting professors will engage in lecturing, teaching and/or research related to the needs of the instructional and research programs of the host institution.
Visiting Scholars and Professional Staff

Individuals nominated by one institution to receive special training in research and teaching or to pursue a specific area of scholarship at the other shall, subject to the approvals required by the host institution, be invited to join the appropriate unit as a visiting scholar.

2.2. Joint Workshops

Joint research and teaching workshops will bring together junior scholars and esteemed faculty from both host universities on a regular basis. Two initial workshops will serve to identify potential overlapping interests, in order to accordingly match up groups or individuals from both sides for further joint programs. The duration of each workshop is up to one week. The number of participants in each workshop will range between 12 to 40.

2.3. Visiting Scholar Workshops

Junior and esteemed scholars from each host university will travel periodically to present their cutting-edge ideas, preliminary findings and working papers. These individual seminars will cross-fertilize more advanced, more interdisciplinary ideas by intentionally tackling diverse topics. While only some of the idea presented will help other activities or mature into a new project, such unstructured presentations and discussions are known to break through academic silos and spur innovation.

2.4. Facilities and Collaboration in Long-term Research

Following the initial exploratory steps, each host university should strive to include scholars from the other counterpart in application for separate and joint research funding.

2.5. Exchange Information, Advice and Best Practices Concerning the Design of Research Laboratories and Centers

Individual talent and efforts are best utilized when an appropriate institutional framework can support long-term, effective and efficient research. As both counterparts envision significant development of cyber-security related research, the experience of creating institutional support will be shared for mutual benefit.

2.6. Scientific Materials

Scientific materials related to the ongoing research and teaching activities shall be exchanged in order to support each counterpart’s individual or cooperative efforts.

MEMORANDUM OF UNDERSTANDING
Tel Aviv University - Indian Institute of Technology Kanpur
A specific plan will be worked out for each activity depending upon the availability of resources.

3. Administrator

The terms of cooperation for each specific project implemented under this MOU shall be discussed and mutually agreed upon in writing by both parties prior to the initiation of that activity.

The conditions of salary and support for each such visitor (professor, scholar, workshop participant etc.) will be specified in a letter of invitation prior to the start of the appointment. Financial arrangements for short visits will be specified in the letter of invitation. Each institution agrees to assist visitors in gaining access to research facilities and laboratories that may be required in the individual’s planned program of study or research.

4. Representatives

The below named officials are representatives of the respective parties responsible for the development and coordination of the specific activities contemplated by this MOU.

For TAU ICRC
Name: Prof. Raanan Rein
Title: Vice President, TAU
Email: raamang.post@macil

Name: Prof. Isaac Ben Israel
Title: Head of ICRC
Email: itzike@post.tmcil

For IITK
Name: Amalendu Chandra
Title: Dean of R&D
Email: dord@iitk.ac.in

5. End of agreement

This MOU constitutes the entire agreement between the parties and may be amended only in writing signed by all parties.
6. Academic
All research activities undertaken by, or under the direction of, faculty who participate in the projects contemplated by this MOU are to be guided by principles of academic freedom. Neither institution shall impose criteria for the exchange of faculty or students which would violate the principles of non-discrimination.

7. Intellectual Property
All IP related legal issues are subject to applicable legal guidelines. In general, each party to this MOU shall own the IP conceived or first reduced to practice solely by its employees or agents. IP conceived or first reduced to practice jointly by employees or agents of both parties shall be jointly owned.

8. Export Control
The parties hereto agree to comply with all applicable national export laws and regulations. Unless authorized by applicable government license or regulation, neither party will directly or indirectly export or re-export, at any time any technical information or software, furnished or developed under this MOU to any prohibited country.

9. Indemnification
TAU ICRC and IITK shall each indemnify and hold harmless the other, its officers, agents and employees, for any and all liability, damages and cost attributable to the negligent acts or omissions of the indemnifying party, its officers, agents and employees while acting in the scope of their employment, and in furtherance of activities described in this Memorandum of Understanding. Students are not employees or agents of TAU ICRC or IITK for purposes of this Agreement.

10. Conduct
Visiting faculty and students must abide by the laws of the host country, and by the regulations of the host university. Students and others participating in programs contemplated by this MOU will be required to provide proof of adequate health insurance valid in the host country and acceptable to the host institution. Each party shall be solely responsible for its own negligent acts, errors, or omissions.
11. Use of Name
Any use of the name TAU ICRC or IITK, including of related logos in publications shall be restricted to activities explicitly covered by this MOU.

12. Language of Use
All communications and proceedings under this MOU shall be conducted in English.

13. Term, Duration, Extension and Termination
This MOU shall become effective upon signature of all parties. This MOU will be effective for a period of five (5) years from the date of the last signature. This MOU shall be reviewed in its final year and may be extended by mutual written agreement of the parties.

This MOU or any Project may be varied or modified by mutual written agreement. Either party will be entitled at any time at its absolute discretion to terminate the MOU or any Project by giving written notice six (6) months beforehand to the other. Such termination will not adversely affect any exchange in effect prior to the effective date of the termination. Each party will ensure that adequate arrangements are made to complete all commitments under active project agreements in process before the MOU expires or is terminated.

For TAU ICRC

Prof. Raanan Rein, Vice President, TAU
Signature: [Signature]
15/8/2016
Prof. Isaac Ben Israel, Head of the ICRC
Signature: [Signature]
15/8/2016

For IITK

Prof. Amalendu Chandra
Signature: [Signature]
21/7/2016

MEMORANDUM OF UNDERSTANDING
Tel Aviv University - Indian Institute of Technology Kanpur
To facilitate bi-lateral academic scientific relationships and to develop cooperative research and teaching projects in selected fields as mutually agreed upon by the two universities, the following list of broad topics is presented as an example to facilitate discussion. The professional participants will select and design joint projects according to the guiding principles of academic research. The terms of cooperation for each specific project implemented under this MOU shall be discussed and mutually agreed upon in writing by both parties prior to the initiation of that activity.

14.1. Security in the design of future complex cyber-physical systems, including IoT and the following sub-sections:

14.1.1. Smart agriculture
14.1.2. Smart city
14.1.3. Water distribution networks
14.1.4. Sewage and water treatment
14.1.5. Electric distribution management

14.2. Development and mechanisms for improved cyber-attack prevention, detection, and mitigation in complex cyber-physical systems, such as:

14.2.1. Identification of security risks in highly-automated systems, including IoT and algorithmic control
14.2.2. Big Data analytics
14.2.3. Machine Learning
14.2.4. Signal Processing
14.2.5. Self-mitigation of security risks in highly-automated systems

14.3. Comprehensive interdisciplinary cybersecurity: integrating political, social, economic, and human factors with core science and engineering disciplines, such as:

14.3.1. Alternative governance models for cybersecurity
14.3.2. Economic externalities and spill-overs of cybersecurity
14.3.3. Political drivers and inhibitors of information technology diffusion and implementation
14.4. 14.4.1. Telecom
14.4.2. Utilities
14.4.3. Transportation

14.5. 14.5.1. privacy-preserving cryptography and cryptanalysis

14.6. 14.6.1. deterrence
14.6.2. The cyber-attacks attribution problem

14.7. 14.7.1. Comparative Innovation Studies
14.7.2. Academic, government and business activities interaction in National Innovation Systems