



RESEARCH AND DEVELOPMENT AGREEMENT

CONTRACT NO. TII/CRP/2040/2021

Between

**TECHNOLOGY INNOVATION INSTITUTE - SOLE
PROPRIETORSHIP LLC**

And

UNIVERSIDADE FEDERAL DE SANTA CATARINA

RESEARCH AND DEVELOPMENT AGREEMENT

UNIVERSIDADE FEDERAL DE SANTA CATARINA, a Brazilian federal autarchy, enrolled with the CNPJ 83.899.526/0001-82, headquartered at Campus Universitário Reitor João David Ferreira Lima, s/n, Florianópolis – SC, Brasil, in this act represented by his Magnificent Rector Prof. Ubaldo Cesar Balthazar (“**University**”)

- and -

TECHNOLOGY INNOVATION INSTITUTE – Sole Proprietorship LLC, a company established under the laws of United Arab Emirates, having its principal offices at Level 3, Aldar HQ, Abu Dhabi, the United Arab Emirates (“**TII**”);

(each a “**Party**” and collectively, the “**Parties**”).

WHEREAS:

- A. The purpose of this Agreement is to set out terms and conditions that the Parties agree to apply to the performance of research under this Agreement.
- B. It is the intention of the Parties that the research contemplated herein, and more specifically described in the Research and Development Tasks in Annex II, is for, amongst other things, the purpose of Post-Quantum Hybrid Signature Scheme (PQ-HSS), Post-Quantum Hybrid Key Establishment (PQ-HKE) Scheme and Integration of PQ-HSS and PQ-HKE into TLS 1.3 and SSHv2
- C. University has the necessary technical expertise, equipment, and infrastructure, and desires to conduct the Research Project in accordance with the terms and conditions of this agreement (“**Agreement**”).

THE PARTIES AGREE AS FOLLOWS:

1. Research Project

- 1.1. The research and development tasks, that the Parties agree will be undertaken pursuant to the research project (“**Research Project**”), which have been more specifically described in **Annex II** of this Agreement, shall be carried out under the direction of Professor Ricardo Felipe Custódio (the “**Principal Investigator**”), a faculty member of University’s Department of Information and Statistics.
- 1.2. In consideration of TII providing the support described in Clause 3 of this Agreement, University will exercise diligence and use its best efforts to perform the tasks of the Research Project, under the direction of the Principal Investigator, and provide TII with any reports or other deliverables required under this Agreement.
- 1.3. The University hereby understands and acknowledges that it is responsible for the adherence of the Principal Investigator and the faculty members and students of University identified as participating in the Research Project (collectively such persons, together with the Principal Investigator, the “**Research Members**”) to the terms of this Agreement. For the avoidance of doubt, University shall be responsible and liable for all acts and omissions of the Research Members and any of its other personnel involved in the performance of the University’s obligations hereunder.

- 1.4. University will conduct the Research Project in accordance with generally accepted professional standards of workmanship and effort at a quality comparable to research performed at major public and private research universities within Brazil. TII understands that all research is experimental in nature and that the outcome of the Research Project is inherently uncertain and unpredictable. TII agrees and acknowledges that the University has not made, and does not make, any representation, guarantee, or warranty, express or implied, regarding the results of the Research Project.
- 1.5. University agrees to promptly advise TII of any proposed change in the employment status of the Principal Investigator and understands that, in the context of the continuation of the Research Project, any such change requires the written approval of TII. If the Principal Investigator ceases to be associated with University or otherwise becomes unavailable to direct the Research Project, TII may at its option request that University replace the Principal Investigator with a qualified person acceptable to TII. In the event a qualified replacement Principal Investigator is not available or acceptable, either Party may choose to terminate the agreement in accordance with clause 2.2.
- 1.6. University agrees to promptly advise TII of any change to any of the Research Members, including providing details of any such replacement person.

2. Term

- 2.1. This Agreement is entered into for a period of thirty (30) months ("**Term**"), which begins on the date of signature of this agreement ("**Commencement Date**"). In the event that the Research Project has not been completed within that one year period, and providing that the University is not otherwise in material breach of this Agreement, University may extend the Term for an additional period of one (1) year by providing written notice to TII of its election to so extending this Agreement. Any further extension of the Term will require an amendment of this Agreement approved and executed by both Parties.
- 2.2. Either Party may terminate this Agreement for any reason upon thirty (30) days' prior written notice to the other Party. Termination of this Agreement by either Party shall not affect the rights and obligations of the Parties accrued prior to the effective date of the termination, and, in the event of a termination by TII for any reason, TII will pay University, subject to the Cost Limit prescribed for the Research Project in clause 3.1 below, for (i) any work performed by University in accordance with the terms of this Agreement up to the effective date of termination and (ii) any non-cancelable expenses incurred by University in preparation for the Research Project and approved in writing by TII prior to the receipt by University of TII's notice of termination.

3. Cost Limit

- 3.1. The project cost shall be set at 100,000.00 (one hundred thousand dollars) **USD** for all personnel-related costs and expenses related to the Research Project (subject to an annual cap on expenses of **USD** 5,000.00 (five thousand dollars)), inclusive of value-added tax and any other applicable taxes, (the "**Fixed Project Cost**") and TII shall not be liable to pay any amounts beyond the Fixed Project Cost that are incurred by University without the prior written approval of TII (with the aggregate of the Fixed Project Cost and all other amounts so approved by TII being referred to as the "**Cost Limit**").
- 3.2. During the term of this Agreement, TII will reimburse the University for the personnel-related costs and expenses incurred in performing the Research Project, calculated on a fair and reasonable basis and in accordance with University usual and customary practices, up to the Cost Limit. University shall submit invoices (together with supporting evidence) as per payment schedule in Annex II. University shall not invoice TII for any amount in excess of the Fixed Project Cost, or for costs and expenses incurred before the Commencement Date of this Agreement, without first obtaining TII's prior written approval.

- 3.3. Equipment purchased out of funds provided hereunder and the cost of which is in excess of USD5,000 shall be exclusively used for the Research Project.

4. General

- 4.1. This Agreement constitutes the entire agreement between the Parties and supersedes all prior oral or written agreements, commitments, or understandings concerning the matters provided for herein.
- 4.2. This Agreement may only be modified by a subsequent written agreement executed by the duly-authorized representatives of the Parties.
- 4.3. If any provision of this Agreement or of any other agreement, document or writing pursuant to or in connection with this Agreement, shall be wholly or partially invalid or unenforceable under applicable law, said provision will be ineffective to that extent only, without in any way affecting the remaining parts or provisions of said agreement, provided that the remaining provisions continue to affect the purposes of this Agreement.
- 4.4. Neither the waiver by any of the Parties hereto of a breach of or a default under any of the provisions of this Agreement, nor the failure of either of the Parties, on one or more occasions, to enforce any of the provisions of this Agreement or to exercise any right or privilege hereunder will thereafter be construed as a waiver of any subsequent breach or default of a similar nature, or as a waiver of any such provisions, rights or privileges hereunder.
- 4.5. Non-performance by a Party, other than payment of any amounts due hereunder by TII, shall not operate as a default under or breach of the terms of this Agreement to the extent and for so long as any such non-performance is due to strikes or other labor disputes; prevention or prohibition by law; the loss or damage to products in transit; an act of god; or war; or other cause beyond the reasonable control of such Party.
- 4.6. The annexes to this Agreement (each an "Annex") form part of this Agreement and shall have the same effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.
- 4.7. University shall not assign, subcontract, or delegate any right or obligation under this Agreement, in whole or in part, without the express prior written consent of TII. Notwithstanding the above, TII shall be free to assign any part of its rights or obligations under this Agreement without the consent of the University.
- 4.8. Each Party undertakes to sign all documents and to do all other acts and things, which may be necessary to give full effect to this Agreement.
- 4.9. Each Party shall pay the costs and expenses incurred by it in connection with the negotiation and entering into this Agreement.
- 4.10. Save as expressly set out in this Agreement, a person who is not a party to this Agreement shall have no right to enforce any of its terms or have any third-party rights of any kind in respect thereof.
- 4.11. The provisions of this Clause 4.11, Clauses 4.10 and 4.12, in each case, of this Agreement and Clauses 2, 3, 4, and 6 of Annex I shall continue to apply notwithstanding termination or expiry of this Agreement.
- 4.12. This Agreement shall be governed by the laws of England and Wales.

4.13. The Parties agree that the any dispute arising out of or in connection with this Agreement shall be referred to and finally and exclusively resolved by arbitration under the London Court of International Arbitration Rules (**Rules**), which Rules are deemed to be incorporated by reference into this Clause. The Parties agree that:

4.13.1. the seat of the arbitration shall be London;

4.13.2. there shall be three (3) arbitrators;

4.13.3. each Party shall nominate one arbitrator and those two arbitrators nominated by the Parties shall jointly nominate the third arbitrator;

4.13.4. the language of the arbitration shall be English;

4.13.5. the award in such arbitration shall be final and binding upon the Parties and judgment may be entered in any court having jurisdiction for its enforcement.



4.14. This Agreement may be signed in any number of counterparts, and each Party may sign one or more counterparts. The counterparts shall together form and be construed as one and the same document.

Executed by the duly authorised signatories of the Parties:

On behalf of **UNIVERSIDADE FEDERAL
DE SANTA CATARINA**

On behalf of **TECHNOLOGY INNOVATION INSTITUTE
- Sole Proprietorship LLC**

Name: Ubaldo Cesar Balthazar
Title: Rector
Date:



Name: Faisal Abdulaziz Al Bannai
Title: Secretary General
Date: May 10th 2021

Name: Ricardo Felipe Custódio
Title: Principal Investigator
Date:

ANNEX I

TERMS AND CONDITIONS

Capitalized words and phrases, and not otherwise defined within this Annex I, shall have such meaning as given to them in the main body of the Agreement.

1. SCOPE OF RESEARCH PROJECT

- 1.1. The scope of the Research Project is determined by the description of the work, as more specifically described in **Annex II** of this Agreement, and shall incorporate, from time to time, any and all amendments, additions and/or extensions to the scope of the Research Project that the Parties may agree to in writing subsequently.
- 1.2. Amendments, additions and/or extensions pertaining to the Research Project, are only binding after having been agreed to in writing by both Parties.
- 1.3. The work described in **Annex II** states how the reporting on the work to be executed is to take place. If the Parties do not prescribe a more detailed reporting mechanism for the Research Project in Annex II, then Principal Investigator will provide TII with semi-annual progress reports within 30 days of the end of each six month period following the Commencement Date, which may be in either oral or written form, or a combination thereof, depending on the nature of the information conveyed. If requested by TII, the Principal Investigator will confirm within a reasonable period of time any oral progress reports with follow-up summary written reports. The Principal Investigator will provide TII a final written report within sixty (60) days after the conclusion of the Research Project, describing the methods used and results obtained together with any other pertinent findings from the Research Project.
- 1.4. When accepting or performing a task under the Research Project to test or develop a working method, a formula, a model or a device, pursuant to this Research Project, University only commits itself to aim, in carrying out the work agreed, for a result that is practicable for TII.
- 1.5. Research into the existence of patent rights of third parties or into the possibility of patenting do not fall within the scope of this Research Project.
- 1.6. The Research Project shall be carried out within the estimated or exact period identified in the main body of the Agreement, subject to any extension period permitted by the Agreement or granted by TII. If the time allotted risks being exceeded, University is obliged to consult with TII regarding this as soon as possible.
- 1.7. If the Research Project includes the delivery of a tangible item, University will not issue any guarantees with regard to this tangible item other than as described in this Agreement.

2. CONFIDENTIALITY

- 2.1. In the course of performing under this Agreement, TII and University may provide to each other, or their respective Authorised Recipients, certain proprietary information, whether orally, in writing or in any other form and whether before or after the date of this Agreement, in connection with the Research Project, the affairs of the other Party, or the clients of the other Party (including for the avoidance of doubt any information the providing Party receives from its clients), and any information acquired by observation by a Party at the offices or premises of the other Party relating to the Research Project or the

- affairs of the other Party together with all analyses, memoranda or other documents or information which contain or reflect or are generated from the information which one Party provides to the other Party or which is obtained by a Party by observation ("**Confidential Information**").
- 2.2. For the purposes of this Clause 2 of Annex I, ("**Authorised Recipient**") shall mean, in relation to each Party, to the extent that they need access to Confidential Information for the purposes of or in connection with the Research Project:
- (a) its respective directors, officers and employees, including Research Members;
 - (b) its auditors and legal advisers; and
 - (c) subject to the prior written consent of the disclosing Party, any other named person.
- 2.3. The Parties will each hold the Confidential Information in strict confidence and will not disclose, copy, reproduce or distribute any of it for any purpose other than a purpose related to the Research Project or to any other person other than an Authorised Recipient, on condition that the Authorised Recipient undertakes not to disclose, copy, reproduce or distribute it to any person who is not an Authorised Recipient or otherwise without the prior written approval of the disclosing Party ("**Provider**"). Each Party will ensure that the confidentiality of the other Party's Confidential Information is safeguarded by adopting at least an equivalent standard as it uses to safeguard its own confidential information, and will require its employees, students and staff members to adhere to such obligation of confidentiality.
- 2.4. Each Party undertakes that it will not, without the prior written consent of the Provider, use any of the Confidential Information for any purpose other than the Research Project.
- 2.5. The following shall be exceptions to the confidentiality undertakings in this Agreement:
- (a) information which at the time of supply is in the public domain;
 - (b) information which subsequently comes into the public domain, except through a breach of the undertakings set out in this Agreement;
 - (c) information that is already in the lawful possession of a Party (as evidenced by written records) without the use or benefit of Confidential Information;
 - (d) information that is independently developed by a Party (as evidenced by written records) without the use or benefit of Confidential Information;
 - (e) information that subsequently comes lawfully into the possession of a Party from a third party, except through a breach of an obligation of confidence in relation to it; or
 - (f) information that is required to be disclosed by law or any governmental or competent regulatory authority with authority over the receiving Party, as long as, and to the extent permissible by law, the disclosing Party supplies a copy of the required disclosure to, and consults in advance with, the Provider on the proposed form, timing, nature and purpose of the disclosure.
- 2.6. Each Party will ensure that each of its respective Authorised Recipients who receive any Confidential Information is aware of and adheres to the terms of this Agreement. The

Parties will each be responsible for any breach of this Agreement by any of their respective Authorised Recipients.

- 2.7. Upon the written request of the Provider, each Party agrees:
- (a) to return to the Provider or destroy all documents containing Confidential Information (other than analyses, memoranda, reports or other documents derived from the Confidential Information) provided to that Party by or on behalf of the Provider;
 - (b) to destroy all copies of any analyses, memoranda or other documents derived from the Confidential Information provided to that Party by or on behalf of the Provider; and
 - (c) to the extent practicable, to expunge all Confidential Information provided to that Party by or on behalf of the Provider from any computer, word processor or other device containing such Confidential Information.
- 2.8. Unless agreed otherwise at the time when the Research Project is commenced, or in connection with the publication of the results of the Research Project, University undertakes to keep the name of TII confidential until one (1) year after the expiry or termination of this Agreement. Unless published in accordance with Clause 2.11 of Annex 1, the same applies to new know-how and data that specifically relates to the Research Project, that has been generated, gained or first put into use within the scope of the Research Project, except in so far as these constitute calculation methods, software and experimental working methods. With regard to inspections, analyses, measurements, or literature searches, no obligation to maintain confidentiality shall apply other than in relation to the actual inspection, analysis, measurement, or literature search and to the outcome of the inspection, analysis or measurement carried out.
- 2.9. Notwithstanding anything to the contrary, University may submit to TII for TII's review, such as TII's Confidential Information as University may wish to include in self-promotional material. TII shall, in its sole discretion i) allow University to use that Confidential Information as provided; ii) revise that Confidential Information as TII may see fit and allow University to use the revised Confidential Information; or iii) refuse to allow University to use that Confidential Information. In the event TII allows University to use either that Confidential Information as provided or as revised by TII, University agrees it shall not expand, abridge, revise or modify that Confidential Information and it shall only use that Confidential Information in the specific format, wording and context as approved by TII.
- 2.10. Subject to the exceptions in this clause 2 of Annex I, each Party undertakes to treat and keep all Confidential Information of the other Party disclosed to it hereunder as confidential throughout the term hereof and for two years thereafter (the "**Standard Confidentiality Period**"). Where a Provider notifies the receiving Party prior to the end of the Standard Confidentiality Period that certain Confidential Information (which Confidential Information shall be specifically identified in that notice) is to remain confidential, then the period of confidentiality in respect thereof shall be extended by a period of two (2) years. Notwithstanding the terms of this clause 2.10 of Annex I, Confidential Information that would be considered as trade-secret under any applicable law shall be kept confidential for the duration of such Confidential Information's treatment as a trade secret under applicable law.
- 2.11. Where the instructional and research rules of the University envisage the publication of research projects undertaken by faculty members, University shall be free to publish the results of the Research Project after providing TII with a sixty (60) day period in which to review each proposed publication in order to (a) identify the patentable subject matter and

(b) to identify any inadvertent disclosure of Confidential Information. Where the patentable subject matter is so identified, the Principal Investigator and University shall grant TII a reasonable additional review period of sixty (60) days for the purpose of the preparation and filing of patent applications pursuant to Clause 4.1 of Annex I. Any further extension will require a subsequent written agreement between TII and University.

- 2.12. Prior written permission by TII is required for the engagement of third parties outside the University for the execution of the Research Project in order to ensure that, amongst other things, there are no foreseeable risks with regard to confidentiality.
- 2.13. Proposals for new research or development, as well as proposals for amendment or extension of the Research Project, may be issued from time to time by University, under the condition that the exclusive existing know-how of the University, not including any Research Project IP, is strictly used by TII solely in order to form an opinion about the new proposals from University.
- 2.14. University shall refrain from accepting research and development tasks that are within the scope of the Research Project, from third parties, during the term of this Agreement. Further, University shall not accept funding from third parties to carry out the Research Project, or another project covering the same research, during the term of this Agreement.

3. RIGHTS TO RESULTS AND INTELLECTUAL PROPERTY

- 3.1. All existing know-how or existing intellectual property, ("**Background IP**") is the separate intellectual property of TII or University, respectively, and is not affected by this Agreement. This Agreement shall not be construed as implying that either Party hereto shall have the right to use Background IP of the other Party in connection with this Agreement, except as otherwise expressly provided herein
- 3.2. Title to any invention, whether or not patentable, conceived or first reduced to practice, or title to and the copyright in any copyrightable material, or any software, first produced and composed, in performance of the Research Project solely by TII's personnel without significant involvement of University's personnel ("**TII Research Project IP**") shall remain with TII. TII Research Project IP shall not be subject to the terms and conditions of this Agreement.
- 3.3. Title to any invention conceived or first reduced to practice, or title to and copyright in any copyrightable material, or any software, first produced and composed, in performance of the Research Project solely by University's personnel without significant involvement of TII's personnel ("**University Research Project IP**") shall remain with University. If requested by TII, University shall grant to TII a perpetual, fully-paid, royalty-free, world-wide, non-exclusive license to use in any field of interest University's Research Project IP, including, without limitation, the right to sublicense either commercially or non-commercially in any jurisdiction.
- 3.4. The Parties shall have joint title to any invention, whether or not patentable, conceived or first reduced to practice, or joint title and copyright in any copyrightable material, or any software, first produced and composed, jointly by University's personnel and TII's personnel in the performance of the Research Project and which are not TII Research Project IP or University Research Project IP (each a "**Joint Research Project IP**"). If requested by TII, University shall grant to TII a perpetual, fully-paid, royalty-free, worldwide, non-exclusive license to use in any field of interest University's share of the Joint Research Project IP, including, without limitation, the right to sublicense either commercially or non-commercially in any jurisdiction.

- 3.5. University will promptly disclose to TII in writing any University Research Project IP or Joint Research Project IP arising during the Research Project performed hereunder. Such disclosure shall be sufficiently detailed for TII to assess the commercial viability of the technology. Upon University's receipt of a written invention disclosure from a Research Member describing any University Research Project IP or Joint Research Project IP, University shall notify TII in writing and provide all available, pertinent information for evaluation and exercise by TII of any option available to it. Any disclosure, and/or related materials, provided by the University to TII, pursuant to this Clause 3.5 of Annex I, shall be treated, under Clause 2 of Annex I, as University Confidential Information whether or not such information or material is marked with an appropriate stamp or legend.

4. PROTECTION OF KNOW-HOW AND INTELLECTUAL PROPERTY

- 4.1. Each Party shall have the right to file and prosecute any patent application in connection with any Joint Research Project IP for itself and on behalf of the other Party. TII shall have the sole right to file and prosecute a patent application in connection with any TII Research Project IP. University shall have the sole right to file and prosecute a patent application in connection with any University Research Project IP.
- 4.2. All expenses incurred in obtaining, enforcing, and maintaining any patent, copyright, or marks on TII Research Project IP, University Research Project IP or Joint Research Project IP ("**Research Project IP**"), including any licensing arrangements entered into between the Parties in respect of Research Project IP, shall be borne solely by TII.
- 4.3. University will, at the written request of TII, during or following the term of this Agreement, reasonably cooperate with TII in the protection of intellectual property licensed under this Agreement.
- 4.4. Without TII's prior written approval, no Background IP will be used in connection with the Research Project if it could lead to any results of the Research Project (including any deliverable) containing, interfacing with, requiring, being linked to and/or making use of any Background IP in order to put into practice and/or commercialise such results of the Research Project.
- 4.5. If University's Background IP is required by TII in order to reduce to practice the TII Licensed Research Project IP, then University will, to the extent that such rights are capable of being so licensed, grant to TII a perpetual, fully-paid, royalty-free, worldwide, non-exclusive license to University's Background IP to use such IP for purposes of permitted use under this Agreement.
- 4.6. In relation to any software forming part of TII Licensed Research Project IP, University will not be entitled to (and the University undertakes not to permit or allow any person to) release it as open-source nor make it generally available to third parties, in each case, without TII's prior written approval (exercisable at TII's sole discretion).

5. PRICE AND PAYMENT

- 5.1. In accordance with the main body of the Agreement, the Cost Limit represents the maximum amount payable for the Research Project.

- 5.2. Unless stated otherwise, all amounts to be paid to the University in the Agreement are inclusive of value-added tax and any other taxes that may be applicable in the jurisdiction of the University.
- 5.3. University shall be entitled to submit periodic invoices every six months.
- 5.4. TII shall pay any undisputed invoices, up to the Cost Limit, in the currency indicated herein, within 45 days after receipt of invoice.
- 5.5. TII reserves the right to audit the University's records, equipment purchased and other costs and expenses so as to determine acceptable use of funds.

6. LIABILITY

- 6.1. University and/or persons used and/or engaged by University in connection with the Research Project are not liable for any loss that TII suffers through its application or use of any Research Project IP or any other result of the work performed by University in relation to the Research Project, except in case of wilful misconduct or gross negligence or recklessness on the part of University and/or of any person or persons that University uses and/or engages in connection with the Research Project.
- 6.2. TII indemnifies University and/or persons used and/or engaged by University for the execution of the Research Project against all claims by third parties on account of losses incurred by such third parties arising from the application or use of any Research Project IP or any other result of the work of University in relation to the Research Project by TII or by another party to whom TII has made that result available. Such indemnification does not apply in case of wilful misconduct or gross negligence or recklessness on the part of University and/or on the part of any person or persons whom the University uses and/or engages for the execution of the Research Project.
- 6.3. TII is liable for damage that University, and/or persons that University uses and/or engages for the execution of the Research Project, suffer during their stay on the premises of TII or during the stay required or requested by TII on premises of third parties in connection with the Research Project unless the damage is caused by recklessness, wilful misconduct or gross negligence on the part of University and/or persons that University uses and/or engages for the execution of the Research Project. University and/or persons that University uses and/or engages are obliged to comply with the safety regulations that apply on the aforementioned premises.
- 6.4. University bears no risk for damage that TII and/or its personnel suffer during and as a result of their stay on the premises and in the buildings of University unless the damage is caused by recklessness, wilful misconduct, or gross negligence on the part of University and/or persons that University uses and/or engages for the execution of the Research Project. TII and/or its personnel are obliged to comply with the safety regulations that apply on the premises and in the buildings of the University.
- 6.5. Neither Party accepts liability to the other Party for any loss that arises from the fact that the results of the Research Project are not patentable or because the rights of third parties are infringed by application of the results of the Research Project by the other Party.
- 6.6. University accepts no liability for losses that result from defects of objects delivered to the University that are passed onward by University to TII, unless and to the extent that University can hold its supplier liable for such loss.

- 6.7. In no case shall either Party be liable for indirect or consequential loss or damage, including but not limited to loss of profit, revenue or contracts.
- 6.8. In connection with any liability of TII to University under this Clause 6 of Annex I, University undertakes to notify TII upon learning of any claim or threatened claim in relation to any actual or potential liability, losses, damages, costs, or expenses and to cooperate with TII in every proper way in the defense or settlement thereof at TII's request and expense. TII shall be entitled to manage any such claims process, but shall not dispose of or settle any claim admitting liability on the part of the University without the University's prior written consent.

7. MISCELLANEOUS

- 7.1. If TII has not made arrangements within two months after the date of the closing invoice for the return of goods that were made available to the University by TII in connection with the Research Project, then any related costs reasonably incurred by University in returning the goods to TII will be payable by TII.
- 7.2. For work in connection with the Research Project on the premises of TII, TII shall, if University requests such on a timely basis, make assisting personnel and auxiliary equipment available to University.
- 7.3. If any Party (the "**Defaulting Party**") is in breach of a key obligation under the Agreement (a "**Major Breach**") or suffers a Solvency Event, then the non-defaulting Party (the "**Non-Defaulting Party**") shall have the right to immediately terminate the Agreement for such Major Breach or Solvency Event upon giving a written termination notice to the Defaulting Party, provided that in relation to that Material Breach the Defaulting Party has been given by the Non-Defaulting Party a written notice that references this Clause 7.3 of Annex I, identifies the breach in reasonable detail and requests the Defaulting Party to rectify the same by a specified date (which date allows the Defaulting Party a reasonable period within which to cure the Major Breach). In this Agreement, "**Solvency Event**" means, in relation to any Party, any corporate action, legal proceedings or other procedure or step that is taken in relation to winding up, dissolution, reorganisation (other than a solvent reorganisation), the appointment of a liquidator, receiver, administrator or administrative receiver or any analogous procedure or step is taken in any jurisdiction.
- 7.4. The Parties hereby agree that they are at all times each acting as independent contractors. Nothing in this Agreement will be construed or deemed to create a relationship of employer and employee, partner, joint venturer, or principal and agent between TII and University, its faculty/faculties, employees, agents or officers. Except as expressly set forth in this Agreement, TII shall neither have nor exercise any control or direction over the methods by which University conducts the research and other work under this Agreement.
- 7.5. The officers, members of faculty/faculties, employees, fellows, trainees, and students of each Party participating in the Research Project will in no sense be considered employees of the other Party. Neither Party assumes and will not assume any liability under any law relating to worker's compensation by reason of any of its representatives participating in the Research Project, receiving training, or traveling pursuant to this Agreement. Nothing in this Agreement will be construed as a waiver by any Party of any rights it may have under any applicable law governing injury to workers.

ANNEX II

RESEARCH PROJECT TASK AND SCOPE

Capitalized words and phrases, and not otherwise defined within Annex II, shall have such meaning as given to them in the main body of the Agreement and otherwise as given to them in Annex I.

DETAILS OF RESEARCH

1. **RESEARCH FOCUS:** Study the design and security properties of hybrid key-establishment protocols and hybrid signature schemes, considering the combination of currently used algorithms and post-quantum algorithms submitted to the NIST standardization process.

Hybrid Cryptographic Protocols

Quantum-resistant key-exchange/encapsulation mechanisms as well as digital signatures will be standardized in the upcoming years. The pace at which industry will integrate these new standards will depend on several factors, namely on (a) how conservative the defined standards are (i.e., how well understood/studied the schemes are); (b) what are the security requirements of a specific product/use case, and (c) how well fitted are the new standards in terms of performance, computational complexity and sizes/memory footprint when replacing classical/conventional schemes.

According to NIST, a hybrid key establishment mode (referred to elsewhere by other names, such as a composite mode) is a key-establishment scheme that is a combination of two or more components consisting of cryptographic key-establishment schemes. The desired property is that keys derived by a hybrid key-establishment scheme remain secure if at least one of the component schemes is secure. The case of interest is when one of the components of the hybrid mode is, for example, NIST-approved (i.e., a discrete-logarithm based scheme from NIST SP 800-56A or an integer-factorization scheme from SP 800-56B, or any other valid alternative) and another component is a post-quantum cryptography scheme.

A hybrid signature consists of two (or more) signatures of a common message (also referred to as dual signature). The verification of hybrid signatures requires all of the signatures to be individually successfully verified. In this case, one of the signature schemes could be a NIST-approved signature scheme as specified in FIPS 186 (or any other valid alternative) and the other one/s could be quantum-resistant.

In this project, we would like to focus on TLS and SSH protocols, with the aim of studying the design considerations and security properties of:

1. How to negotiate the use of multiple algorithms for hybrid key establishment;
2. How to combine multiple symmetric keys;
3. How to add hybrid authentication via digital signatures;
4. How to integrate hybrid schemes in TLS 1.3 and SSHv2.

A good reference to start: E. Crockett, C. Paquin, and D. Stebila. "Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH"

The security of such protocols should be assessed by using formal verification tools. Implementation and performance challenges (such as latencies, size impact, etc.) should be clearly highlighted in theoretical set-ups and also applied to a realistic client to server/server to client scenarios.

There are a series of initiatives for protocol formal verification. We should highlight the use of automated protocol verification tools such as ProVerif and other specialised tools. We know there are a series of different implementations that are well-established and well understood regarding TLS and SSH protocols. We want to start from that and add two or more key-establishment/signatures into the description and perform the same sort of verification that already works for the previous single-key-establishment/signature

version of the protocols. The main challenge of conducting such sort of verification is the actual description and implementation of the post-quantum cryptography primitives into the automated protocol verification tools.

FIPS Compliance

FIPS Compliance is not a requirement in this project, but it's useful to take the below into account when building Hybrid protocols.

Current NIST standards, which were not necessarily designed to provide post-quantum security, can accommodate several hybrid key establishment constructions in "FIPS mode," as defined in FIPS 140. For example, assume that the value Z is a shared secret that was generated within a NIST-approved cryptographic scheme and that a value T is generated or distributed through another scheme(s), which could be the output of a key encapsulation method (KEM). The following are the different ways to incorporate the value T in the key derivation procedure to achieve a hybrid mode which is permitted by current standards:

- 1) For any one-step key derivation method that is specified in SP 800-56C, an input defined as SuppPrivInfo can be included in an (optional) FixedInfo field, and T may be included in that field;
- 2) In any of the key derivation methods specified in SP 800-56C, whether one-step or extraction-then-expansion, the value T may be included in the salt field. Additionally, NIST plans to incorporate a cleaner, and therefore preferable, hybrid key establishment construction in a future revision of SP 800-56C;
- 3) In any of the key derivation methods specified in SP 800 - 56C, the revision would permit a concatenation of Z and T, e.g., Z||T, to serve as the shared secret instead of Z. This would require the insertion of T into the coding for the scheme and the FIPS 140 validation code may need to be modified.

FIPS-compliance hybrid digital signatures can be achieved as far as one of the digital signatures used is specified in FIPS 186.

Milestones

Literature Review and Evaluation

First and foremost, we will list desirable properties of existing hybrid schemes, such as usability, compatibility, security and performance. We must then determine an evaluation metric to filter, rank and compare works in the literature. This will eventually produce a detailed report that we intend to publish as a survey. Namely, we would like to understand what has been achieved so far and what remains to be done.

Post-Quantum Hybrid Signature Scheme (PQ-HSS)

Starting at what we believe is the cornerstone for our goals, we would like to further develop PQ-HSS. This result may be useful in the upcoming milestones where authentication may use digital signatures for authentication. We will establish a framework, such as compatible technologies, algorithms and standards, to elaborate on a novel approach. We aim to discuss and analyze the security of our strategy using automated formal verification tools, such as *proverif*, considering classic and quantum threat models.

Post-Quantum Hybrid Key Establishment Scheme (PQ-HKE)

We would like to further develop PQ-HKE. As for signatures, we will establish a framework to elaborate a novel approach to PQ-HKE. We also aim to discuss and analyze the security of our strategy using automated formal verification tools, such as *proverif*, considering classic and quantum threat models. Moreover, following the 2020 revision of NIST recommendation SP 800-56C, we aim to find the best alternatives concerning hybrid shared secret key-derivation. Namely, we believe that a symmetric key derived from the concatenation of two or more distinct secret pieces should be further discussed and

developed. Furthermore, we review our new contributions and the ones available in the literature to understand how to enable authenticated key establishment using PQ-HSS.

Integration of PQ-HSS and PQ-HKE into TLS 1.3 and SSHv2

Our goal is to develop a software implementation to integrate PQ-HSS and PQ-HKE to TLS and SSH protocols. There are many open-source libraries available that are widely used and well maintained, providing support for these protocols. We intend to patch these libraries, such as OpenSSL and OpenSSH, with mechanisms and support for our methods.

Delivery Schedule

We project a delivery package to be completed every two months, allowing enough creative period. Each package will be in the form of a **technical report**, usually aiming towards publication material. That is, we propose to write reports that may eventually produce one or more papers to be submitted to internationally renowned conferences or journals.

Literature Evaluation

1. Establish evaluation metrics (if not available then propose),
2. Review PQ-HSS;
3. Review PQ-HKE and review hybrid TLS/SSH Implementations;
4. Filter, rank, and evaluate related work.

Post-Quantum Hybrid Signature Scheme

5. Establish technologies, algorithms, properties, and standards;
6. Design PQ-HSS Prototype;
7. Evaluate and compare to related work.

Post-Quantum Hybrid Key Establishment Scheme

8. Establish technologies, algorithms, properties, and standards;
9. Design PQ-HKE Prototype;
10. Evaluate and compare to related work.

Integration of PQ-HSS and PQ-HKE into TLS 1.3 and SSHv2

11. Establish compatible technologies, frameworks, libraries;
12. Library patch development, evaluation and comparison to related work.

TIMELINE, RESOURCES, AND MISCELLANEOUS

Collaborating Parties	Technology Innovation Institute - Sole Proprietorship LLC Universidade Federal De Santa Catarina
Timeline	30 months (subject to extension in accordance with the Agreement)
Publications Requirement	2 Publications in top Conferences (Joint between TII and University) 1 White Paper (Joint between TII and University)
Prototyping and Platforms	Platform Specific Implementations
Resources	1 Postdoc student (University) 1 Ph.D. student (University) 1 Master student (University) 1 Undergraduate student (University) Prof. Ricardo Felipe Custódio (University) Prof. Jean Everson Martina (University) 2 Resources from TII (Names TBD)

Logistics	Bi-weekly [Zoom/Skype/etc] Meeting [[Quarterly]/[Semi-annual report]] as specified in Clause 1.3 of Annex I to be discussed in person[; To be [negotiated] in a good faith by both Parties.]
------------------	---

FUNDING

Total Research Funds	Total US\$ 100,000.00 Payment schedule – the amount in USD: <ul style="list-style-type: none"> ● US\$ 20,000.00 –Signature of Agreement (advance payment) payable within thirty (30) days of the Commencement Date ● US\$ 40,000.00 – Payable upon 6 deliveries and within 12 months of the Commencement Date ● US\$ 40,000.00 – Payable upon 6 deliveries and within 24 months of the Commencement Date
Expenses / Travels / Conferences	Expenses for travels and conferences related to the project (travel, accommodation and per diem) will be covered by TII subject to TII approval.
Systems and Tools	Sponsored by TECHNOLOGY INNOVATION INSTITUTE - Sole Proprietorship LLC

ROADMAP

First Year Activities	1	2	3	4	5	6	7	8	9	10	11	12
1. Evaluation Metrics Technical Report.	X	X										
2. Hybrid Schemes Review Technical Report.		X	X	X								
3. Hybrid Schemes Evaluation Technical Report.				X	X	X						
4. Post-quantum Hybrid Signature Scheme framework Technical Report.						X	X	X				
5. Post-quantum Hybrid Signature Scheme Prototype.							X	X	X	X		
6. Post-quantum Hybrid Signature Scheme Prototype Evaluation Technical Report.										X	X	X
Second Year Activities	1	2	3	4	5	6	7	8	9	10	11	12
7. Post-quantum Hybrid Key Establishment framework Technical Report.	X	X										
8. Post-quantum Hybrid Key Establishment Prototype.		X	X	X								
9. Post-quantum Hybrid Key Establishment Prototype Evaluation Technical Report.				X	X	X						

10. TLS and SSH implementation Technical Report.					X	X	X	X	X			
11. TLS and SSH implementation Library Patch.							X	X	X	X	X	X
Third Year Activities	1	2	3	4	5	6	-	-	-	-	-	-
12. Evaluation of Hybrid Key Agreement Protocols.	X	X	X									
13. Research Group meetings with report production.			X	X	X	X						