NIST has entered into two patent license agreements to facilitate adoption of NIST's announced selection of Public-Key Encryption PQC algorithm CRYSTALS-KYBER. NIST and the licensing parties share a desire, in the public interest, the licensed patents be freely available to be practiced by any implementer of the CRYSTALS-KYBER algorithm as published by NIST.

The licenses cover a patent portfolio privately owned by a US entity (US Portfolio)[1] and a portfolio controlled by French institutions (French Portfolio).[2]

The licenses were drafted such that any implementer of the CRYSTALS-KYBER algorithm as published by NIST receive the benefits of a grant to the licensed patents within the scope of a field of use limited to implementing CRYSTALS-KYBER as a PQC algorithm. The licensors agreed, on a royalty-free basis, to place into abeyance any right of enforcement of the licensed patents against any implementer or end-user of the algorithm.

Relevant language (with modifications for readability) from the licenses regarding the scope of use permitted to implementers of the CRYSTALS-KYBER algorithm follow. Where language differs between the licenses in a manner which could be read to influence the rights of implementers, the language of both licenses is presented.

US Portfolio	French Portfolio
1.3 "IMPLEMENTER" shall mean any entity, person, company, organization, foundation, or business, whether private, public, or governmental, that implements the PQC ALGORITHM in paragraph 1.11 for any purpose that complies with the license granted in paragraph 2.1, whether such implementation is for research, teaching, and other non-commercial purposes or for the purpose of commercial manufacture, distribution, or provision of services or products for a fee.	1.3 "IMPLEMENTER" shall mean any entity, person, company, organization, foundation, or business, whether private, public, or governmental, that implements the PQC ALGORITHM in paragraph 1.11 for any purpose, whether such implementation is for research, teaching, and other non-commercial purposes or for the purpose of commercial manufacture, distribution, or provision of services or products for a fee.
1.5. "LICENSED PRODUCTS" shall mean any apparatus or composition encompassed within the scope of a claim in the LICENSED PATENT and implementing the PQC ALGORITHM, and shall also include a	1.5. "LICENSED PRODUCTS" shall mean any apparatus or composition encompassed within the scope of a claim in the LICENSED PATENTS and shall also include a product that was manufactured, at least in part, by a

[1] U.S. Pat. No. 9,246,675 and all related patents and applications.

[2] EP App. No. 11712927; EP Pat. No. 2537284; French Pat. App. No. 1051190, French Pat. No. 2956541; PCT App. No. PCT/FR2011/050336; U.S. Pat. App. No. 13/579,682; U.S. Pat. No. 9,094,189; and all related patents and applications.

product that was manufactured, at least in part, by a process encompassed within the scope of a claim in the LICENSED PATENT that has not been held not patentable, invalid, or unenforceable by an unappealed or unappealable judgment of a court of competent jurisdiction or governmental administrative body.	process encompassed within the scope of a claim in the LICENSED PATENTS that has not been held not patentable, invalid, or unenforceable by an unappealed or unappealable judgment of a court of competent jurisdiction or governmental administrative body.
1.6. "LICENSED PROCESSES" shall mean any process that implements the PQC algorithm and, in the course of being practiced, would be encompassed within the scope of a claim in the LICENSED PATENT that has not been held not patentable, invalid, or unenforceable by an unappealed or unappealable judgment of a court of competent jurisdiction or governmental administrative body.	1.6. "LICENSED PROCESSES" shall mean any process that, in the course of being practiced, would be encompassed within the scope of a claim in the LICENSED PATENTS that has not been held not patentable, invalid, or unenforceable by an unappealed or unappealable judgment of a court of competent jurisdiction or governmental administrative body.
1.7. "LICENSED USES" shall mean any method encompassed within the scope of a claim in the LICENSED PATENT and implementing the PQC ALGORITHM that has not been held not patentable, invalid, or unenforceable by an unappealed or unappealable judgment of a court of competent jurisdiction or governmental administrative body.	1.7. "LICENSED USES" shall mean any method encompassed within the scope of a claim in the LICENSED PATENTS that has not been held not patentable, invalid, or unenforceable by an unappealed or unappealable judgment of a court of competent jurisdiction or governmental administrative body.

1.8. "LICENSED TERRITORY" shall mean worldwide wherever a VALID CLAIM exists.

1.9. "VALID CLAIM" shall mean: (a) a claim of an issued and unexpired patent within the LICENSED PATENTS that has not been (i) held permanently revoked, unenforceable, unpatentable or invalid by a decision of a court or governmental body of competent jurisdiction, unappealable or unappealed within the time allowed for appeal, (ii) rendered unenforceable through disclaimer or otherwise, (iii) abandoned, or (iv) permanently lost through an interference or opposition proceeding without any right of appeal or review; or (b) a pending claim of a pending patent application within the LICENSED PATENTS that has been asserted and continues to be prosecuted in good faith where such claim has been pending for a period of ten years or less.

1.10. "FIELD OF USE" shall mean any implementation of the PQC ALGORITHM in 1.11.

US Portfolio	French Portfolio
1.11. "PQC ALGORITHM" shall mean: (a) any standard prescribed by NIST in a NIST Special Publication or Federal Information Processing Standard that is based on the CRYSTALS-KYBER public-key encryption and key-establishment algorithm selected by NIST under the announcement for submission of candidate algorithms for public-key post-quantum standards published in volume 81 page 92787 of the United States Federal Register on December 20, 2016, available as of the EFFECTIVE DATE at https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms, or a subsequent such NIST announcement; (b) a documentary standard set by a standards development organization (SDO) or standards setting organization (SSO); and (c) a government regulation or statute, wherein for each instance of (b) and (c) of this paragraph, only to the extent identical with parameters of the standard prescribed by NIST, and NIST will use reasonable efforts to have a citation to the standard prescribed by NIST included in each instance of (b) and (c) of this paragraph.	1.11. "PQC ALGORITHM" shall mean a post-quantum cryptography algorithm selected by NIST under the announcement for submission of candidate algorithms for public-key post-quantum standards published in volume 81 page 92787 of the United States Federal Register on December 20, 2016, available as of the EFFECTIVE DATE at: https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms, or a subsequent such NIST announcement, and any standard based on a selected post-quantum cryptography algorithm as may be prescribed in a NIST Special Publication, Federal Information Processing Standard, a documentary standard set by a standards developing organization (SDO) or standards setting organization (SSO), or a governmental regulation or statute.

2.1. LICENSORS, on behalf of themselves and any successors and/or assigns, grant to LICENSEE an exclusive, non-transferable, fully paid-up, and irrevocable license, with the right to grant sublicenses,[3] under all claims of the LICENSED PATENTS:

(a) to make, have made, use, sell, offer for sale, lease, import, export or otherwise dispose of the LICENSED PRODUCTS,

(b) to practice the LICENSED PROCESSES, and

(c) to practice the LICENSED USES,

[3] The Algo Consulting, Inc. agreement additionally contains terms limiting sublicensees to the FIELD OF USE.

in the LICENSED TERRITORY.

2.2. LICENSORS agree that this Agreement extends and confers all benefits of the grant in paragraph 2.1 to all IMPLEMENTERS and their end-users on a royalty-free basis for the FIELD OF USE.

2.3. LICENSORS hereby, on a royalty-free basis, place into abeyance any right of enforcement of the LICENSED PATENTS against any IMPLEMENTER and their end-users from any and all actions, causes of action, claims, or demands whatsoever in law or equity as to all claims for patent infringement, direct and/or contributory and/or by inducement or otherwise, which may arise at any time on or after the EFFECTIVE DATE, which could be asserted against any IMPLEMENTER, or against any of IMPLEMENTER's end-users, whether direct or indirect, or immediate or remote, arising out of any implementation of the PQC ALGORITHM commensurate in scope with the FIELD OF USE, including manufacture, having manufactured, use, sale, offer for sale, lease, import, export, or other disposition of the LICENSED PRODUCTS, practice of the LICENSED PROCESSES, and practice of the LICENSED USES in the LICENSED TERRITORY for the FIELD OF USE.

US Portfolio	French Portfolio
2.4. Contingent upon LICENSEE's payment of such portion of the PAYMENT due licensor, LICENSOR hereby releases and discharges LICENSEE, any IMPLEMENTER, whether direct or indirect, or immediate or remote, in the LICENSED TERRITORY, from any and all actions, causes of action, claims, or demands whatsoever in law or equity as to all claims for patent infringement, direct and/or contributory and/or by inducement or otherwise, which LICENSOR has or may have had at any time prior to the EFFECTIVE DATE, which could be asserted against any IMPLEMENTER, or against any of IMPLEMENTER's end-users, whether direct or indirect, or immediate or remote, solely to the extent arising out of any implementation of the PQC ALGORITHM commensurate in scope with the FIELD OF USE, including manufacture, having manufactured, use, sale, offer for sale, lease, import, export, or other disposition of the LICENSED PRODUCTS, practice of the LICENSED PROCESSES, and practice of the LICENSED USES in the LICENSED TERRITORY for the FIELD OF USE. In the case of any lack or delay of	2.4. LICENSORS hereby release and discharge LICENSEE, any IMPLEMENTER, whether direct or indirect, or immediate or remote, in the LICENSED TERRITORY, from any and all actions, causes of action, claims, or demands whatsoever in law or equity as to all claims for patent infringement, direct and/or contributory and/or by inducement or otherwise, which LICENSORS have or may have had at any time prior to the EFFECTIVE DATE, which could be asserted against any IMPLEMENTER, or against any of IMPLEMENTER's end-users, whether direct or indirect, or immediate or remote, arising out of any implementation of the PQC ALGORITHM commensurate in scope with the FIELD OF USE, including manufacture, having manufactured, use, sale, offer for sale, lease, import, export, or other disposition of the LICENSED PRODUCTS, practice of the LICENSED PROCESSES, and practice of the LICENSED USES in the LICENSED TERRITORY for the FIELD OF USE.

federal appropriations to NIST delaying the portion of the PAYMENT due licensor, the releases of LICENSOR in the paragraph shall apply retroactively for any period during this agreement for which a lapse may have occurred due to late payment.	

2.5. LICENSORS provide the GRANTS, RELEASES, DISCHARGES, AND ABEYANCE OF ENFORCEMENT in this Article II with or without notification to any IMPLEMENTER or its end-users.

2.6. LICENSORS reserve the right to (a) use technology covered by any claim of the LICENSED PATENTS; (b) grant rights to the LICENSED PATENTS for uses outside of the FIELD OF USE; and (c) enforce the LICENSED PATENTS for uses outside of the FIELD OF USE.

US Portfolio only: 2.9. For the sake of clarity, any implementation or use of the LICENSED PATENT by LICENSOR, SUBLICENSEE or any of the party that does not meet the definition of the PQC ALGORITHM, including any modification, extension, or derivation of the parameters of the PQC ALGORITHM, is not an implementation or use of the PQC algorithm.