Cover Page

Name of the proposed cryptosystem: Compact-LWE Public Key Encryption Scheme

Principal Submitter:

Name: Dongxi Liu   Email: dongxi.liu@csiro.au   Phone: 61-2-93724152

Organization: Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Postal Address:

CSIRO, Cnr Vimiera and Pembroke Roads, Marsfield, NSW 2122, Australia

Auxiliary Submitters: Nan Li, Jongkil Kim, Surya Nepal

Inventors: Dongxi Liu, Nan Li, Surya Nepal

(Australia provisional patent application no: 2017901941)

Developers: Dongxi Liu, Nan Li, Jongkil Kim, Surya Nepal

Owner: Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Signature of the Submitters

Dongx. Liu

2.D.1 Statement by Each Submitter

I, Dongxi Liu, of CSIRO Cnr Vimiera and Pembroke Roads Marsfield NSW 2122 Australia, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

- □ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE;* ***OR*** *(check one or both of the following):*

  - □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, may be covered by the following U.S. and/or foreign patents: none ;*
  - ☑ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations:* *Australia provisional patent 2017901941* Asymmetric Cryptography and Authentication.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: Dngxi Liu
Title: Senior Research Scientist
Date: 27 Sep 2017
Place: CSIRO, Cnr Vimiera and Pembroke Roads Marsfield, NSW 2122, Australia

2.D.1 Statement by Each Submitter

I, Nan Li, of University of Newcastle University Dr, Callaghan NSW 2308 Australia, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

□ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE;* ***OR*** *(check one or both of the following):*

- □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, may be covered by the following U.S. and/or foreign patents: none ;*
- ☒ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations:* *Australia provisional patent 2017901941* Asymmetric Cryptography and Authentication.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:
Title: Lecturer
Date: 29 Sep 2017
Place: University of Newcastle, University Dr, Callaghan NSW 2308, Australia

2.D.1 Statement by Each Submitter

I, Jongkil Kim, of CSIRO Cnr Vimiera and Pembroke Roads Marsfield NSW 2122 Australia, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

□ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE; **OR** (check one or both of the following):

□ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, may be covered by the following U.S. and/or foreign patents: none ;

☑ I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations: Australia provisional patent 2017901941 Asymmetric Cryptography and Authentication.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:
Title: Postdoctoral Fellow
Date: 27 Sep 2017
Place: CSIRO, Cnr Vimiera and Pembroke Roads Marsfield, NSW 2122, Australia

2.D.1 Statement by Each Submitter

I, Surya Nepal, of CSIRO Cnr Vimiera and Pembroke Roads Marsfield NSW 2122 Australia, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check one):

- □ *I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE;* ***OR*** *(check one or both of the following):*
  - □ *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Compact-LWE, may be covered by the following U.S. and/or foreign patents: none ;*
  - ☑ *I do hereby declare that, to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of my submitted cryptosystem, reference implementation or optimized implementations:* Australia provisional patent 2017901941 Asymmetric Cryptography and Authentication.

I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my cryptosystem, reference implementation or optimized implementations. I also acknowledge and agree that the U.S. Government may, during the public review and the evaluation process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of the standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability).

I acknowledge that NIST will announce any selected cryptosystem(s) and proceed to publish the draft standards for public comment

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my cryptosystem, reference implementation or optimized implementations and the right to use such implementations for the purposes of the public review and evaluation process.

I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized

implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:
Title: Principal Research Scientist
Date: 27 Sep 2017
Place: CSIRO, Cnr Vimiera and Pembroke Roads Marsfield, NSW 2122, Australia

2.D.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner, or each owner's authorized representative, of each patent and patent application identified.

I, Liming Zhu , of CSIRO 13 Garden Street Eveleigh NSW 2015 Australia, am the owner or authorized representative of the owner Commonwealth Scientific and Industrial Research Organisation (CSIRO) (print full name, if different than the signer) of the following patent(s) and/or patent application(s): Australia provisional patent 2017901941 Asymmetric Cryptography and Authentication, and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as Compact-LWE is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard (check one):

without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination, **OR**

[✓ *under reasonable terms and conditions that are demonstrably free of any unfair discrimination.*]

I further do hereby commit and agree to license such party on the same basis with respect to any other patent application or patent hereafter granted to me, or owned or controlled by me, that is or may be necessary for the purpose of implementing the standard.

I further do hereby commit and agree that I will include, in any documents transferring ownership of each patent and patent application, provisions to ensure that the commitments and assurances made by me are binding on the transferee and any future transferee.

I further do hereby commit and agree that these commitments and assurances are intended by me to be binding on successors-in-interest of each patent and patent application, regardless of whether such provisions are included in the relevant transfer documents.

I further do hereby grant to the U.S. Government, during the public review and the evaluation process, and during the lifetime of the standard, a nonexclusive, nontransferrable, irrevocable, paid-up worldwide license solely for the purpose of modifying my submitted cryptosystem's specifications (e.g., to protect against a newly discovered vulnerability) for incorporation into the standard.

Signed:
Title: Research Director, Software and Computational Systems, Data61, CSIRO
Date: 29/11/2017
Place: 13 Garden Street Eveleigh NSW 2015 Australia

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, Dongxi Liu, of CSIRO Cnr Vimiera and Pembroke Roads Marsfield NSW 2122 Australia, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:
Title: Senior Research Scientist
Date: 27 Sep 2017
Place: CSIRO, Cnr Vimiera and Pembroke Roads Marsfield, NSW 2122, Australia

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, Nan Li, of University of Newcastle, University Dr, Callaghan NSW 2308, Australia, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:
Title: Lecturer
Date: 29 Sep 2017
Place: University of Newcastle, University Dr, Callaghan NSW 2308, Australia

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, Jongkil Kim, of CSIRO Cnr Vimiera and Pembroke Roads Marsfield NSW 2122 Australia, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed:
Title: Postdoctoral Fellow
Date: 27 Sep 2017
Place: CSIRO, Cnr Vimiera and Pembroke Roads Marsfield, NSW 2122, Australia

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, , Surya Nepal , of CSIRO Cnr Vimiera and Pembroke Roads Marsfield NSW 2122 Australia, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute copies of, and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process, and implementation if the corresponding cryptosystem is selected for standardization and as a standard, notwithstanding that the implementations may be copyrighted or copyrightable.

Signed: Suryanepal
Title: Principal Research Scientist
Date: 27 Sep 2017
Place: CSIRO, Cnr Vimiera and Pembroke Roads Marsfield, NSW 2122, Australia