

## 2.D.1 Statement by Each Submitter

*I, Partha Sarathi Roy, of 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RaCoSS, 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 RaCoSS; **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 RaCoSS, 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: none.*

*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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.*

Signed:

Title: Researcher

Date: November 15, 2017

Place: 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN

## 2.D.1 Statement by Each Submitter

I, Rui Xu, of 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RaCoSS, 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 RaCoSS; **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 RaCoSS, 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: none.


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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:



Title: Researcher

Date: November 15, 2017

Place: 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN

## 2.D.1 Statement by Each Submitter

*I, Kazuhide Fukushima, of 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RaCoSS, 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 RaCoSS; **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 RaCoSS, 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: none.*

*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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.*

*Signed: Kazuhide Fukushima*  
*Title: Manager*

*Date: November 15, 2017*

*Place: 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN*

## 2.D.1 Statement by Each Submitter

*I, Shinsaku Kiyomoto, of 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RaCoSS, 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 RaCoSS; **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 RaCoSS, 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: none.*

*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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.*

Signed:

Title: Senior Manager

Date: November 15, 2017

Place: 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN

## 2.D.1 Statement by Each Submitter

I, Kirill Morozov, of 3940 N. Elm, Room F283, Denton, TX 76207-7102, USA, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RaCoSS, 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 RaCoSS; **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 RaCoSS, 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: none.

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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:  / Kirill Morozov /  
Title: Associate Professor, University of North Texas, USA  
Date: November 16, 2017  
Place: Denton, TX, USA

## 2.D.1 Statement by Each Submitter

*I, Tsuyoshi Takagi, of 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, JAPAN, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as RaCoSS, 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 RaCoSS; **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 RaCoSS, 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: none.*

*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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.*

*Signed:*

*Title: Professor*

*Date: November 13, 2017*

*Place: 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, JAPAN*



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

The following must also be included:

*I, Shinsaku Kiyomoto, 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, JAPAN, 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 Manager

Date: November 15, 2017

Place: 2-1-15 Ohara, Fujimino-shi, Saitama, 356-8502, Japan