Name of Proposal:

Rainbow

Principal Submitter:

Jintai Ding

email: jintai.ding@gmail.com
phone: 513 556 - 4024
organization: University of Cincinnati
postal address: 4314 French Hall, OH 45221 Cincinnati, USA

Auxiliary Submitters: Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, Bo-Yin Yang

Inventors: c.f. Submitters

Owners: c.f. Submitters

Jintai Ding (Signature)

Additional Point of Contact:

Bo-Yin Yang
email: by@crypto.tw
phone: 886-2-2788-3799
Fax: 886-2-2782-4814
organization: Academia Sinica
postal address: 128 Academia Road, Section 2
Nankang, Taipei 11529, Taiwan

2.D.1 Statement by Each Submitter

I, _____ Jintai Ding____, of 8770 Wellerstation Dr, Cincinnati, OH 45249, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____Rainbow____, 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 ____ (print name of cryptosystem)____; **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 ____Rainbow____, may be covered by the following U.S. and/or foreign patents: _____ US7961876, US7158636 _____ ;

☒ 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: 15/562,034 .

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: 11.2.2017
Place: Cincinnati

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, __Jintai Ding_____ , of 8770 Wellerstation Dr, Cincinnati, OH 45249______ , am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and/or patent application(s): __US7961876, US7158636, 15/562,034 , and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as) _Rainbow______ 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: Professor
Date: 11.2.2017
Place: Cincinnati

2.D.1 Statement by Each Submitter

I, ______Albrecht Petzoldt____, of 439 West Side Drive, Gaithersburg, MD20878, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____Rainbow____, 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 Rainbow____;* ***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 ___ ___, may be covered by the following U.S. and/or foreign patents: _____ __ ;*

□ *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:*

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: A Petzoldt
Title: Dr.
Date: 11.2.2017
Place: Cincinnati

2.D.1 Statement by Each Submitter

I, ___Dieter Schmidt___, of 145 Aberdeen Cir. Springboro, OH 45066, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____Rainbow____, 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 Rainbow____;* ***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 ___ ___, may be covered by the following U.S. and/or foreign patents: _____ __ ;*

□ *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:*

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

2.D.1 Statement by Each Submitter

I, _____Bo-Yin Yang_____, of ___128 Sec. 2 Academia Road, IIS, Taipei, Taiwan , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____Rainbow__ 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 Rainbow____;* ***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 ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;*
- □ *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: _____ (describe and enumerate or state "none" if applicable) ______.*

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: Research Fellow
Date: 2017.11.09
Place: Institute of Information Science, Academia Sinica

2.D.1 Statement by Each Submitter

I, Ming-Shing Chen , of N415,IIS,AS,No.128,2nd Sec.,Academic Rd.,Nangang Dist.,Taipei City,Taiwan , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Rainbow, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that :

- *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 Rainbow.*

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: Ming-Shing Chen
Title: Research Assistant
Date: 9th, Nov., 2017
Place: ITS, AS, Taipei, Taiwan

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

The following must also be included:

I, Ming-Shing Chen , N415,IIS,AS,No.128,2nd Sec.,Academic Rd.,Nangang Dist.,Taipei City,Taiwan , 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: Ming-Shing Chen
Title: Research Assistant
Date: 9th. Nov. 2017
Place: IIS, AS, Tapei, Taiwan

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

The following must also be included:

I, _____ Bo-Yin Yang _____ , 128 Section 2 Academia Road, IIS, Taipei, Taiwan , am the owner or authorized representative of the owner 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: Boyin Yang
Title: Research Fellow
Date: 2017.11.09
Place: Institute of Information Science, Academia Sinica

2.D.1 Statement by Each Submitter

I, Ming-Shing Chen , of N415,IIS,AS,No.128,2nd Sec.,Academic Rd.,Nangang Dist.,Taipei City,Taiwan , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Rainbow, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that :

- *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 Rainbow.*

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: Ming-Shing Chen
Title: Research Assistant
Date: 9th, Nov., 2017
Place: IIS, AS., Taipei, Taiwan

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

The following must also be included:

I, Ming-Shing Chen , N415,IIS,AS,No.128,2nd Sec.,Academic Rd.,Nangang Dist.,Taipei City,Taiwan , 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: Ming-Shing Chen
Title: Research Assistant
Date: 9th, Nov. 2017
Place: IIS, AS, Taipei, Taiwan

2.D.1 Statement by Each Submitter

I, _____Bo-Yin Yang_____, of ___128 Sec. 2 Academia Road, IIS, Taipei, Taiwan , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____Rainbow 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 Rainbow____; **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 ____ (print name of cryptosystem)____, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state "none" if applicable)_____ ;
- □ 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: _____ (describe and enumerate or state "none" if applicable) ______.

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: Research Fellow
Date: 2017.11.09
Place: Institute of Information Science, Academia Sinica

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

The following must also be included:

I, _____ Bo-Yin Yang _____ , 128 Section 2 Academia Road, IIS, Taipei, Taiwan , am the owner or authorized representative of the owner 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: Bo-Yin Yang
Title: Research Fellow
Date: 2017.11.09
Place: Institute of Information Science, Academia Sinica