2.D.1 Statement by Each Submitter

I,_____Koichiro Akiyama_____, of_____1, Komukai-Toshiba-cho, Kawasaki, Kanagawa, Japan_____, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____Giophantus_____, 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____Giophantus_; **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_____Giophantus_____, 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, 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: Koichiro Akiyama

Title: Chief Research Scientist

Date: March 29 2018

Place: Kawasaki, Japan

2.D.1 Statement by Each Submitter

I,_____Yasuhiro Goto_____, of_____1-2 Hachiman-cho, Hakodate, Hokkaido, Japan_____, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____Giophantus_____, 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_____Giophantus_; 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, 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: Professor

Date: March 30, 2018

Place: 1-2 Hachiman-cho, Hakodate, Hokkaido, Japan

2.D.1 Statement by Each Submitter

I,_____Goichiro Hanaoka_____, of_____2-3-26, Aomi, Koto-ku, Tokyo, Japan_, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____Giophantus_____, 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____Giophantus_; **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, 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: Goichiro Hanaoka

Title: Leader, Advanced Cryptosystems Research Group, AIST

Date: Apr. 2, 2018

Place: Tokyo, Japan

2.D.1 Statement by Each Submitter

I,_____Yasuhiko Ikematsu_____, of_7-3-1, Hongo, Bunkyo-ku, Tokyo, Japan_____, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as_Giophantus___, 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____Giophantus_; **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_____Giophantus_____, 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, 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: Yasuhiko Ikematsu

Title: project researcher

Date: April 2, 2018

Place: Tokyo, Japan

2.D.1 Statement by Each Submitter

I,_____Koji Nuida_____, of_____7-3-1 Hongo, Bunkyo-ku, Tokyo,_ Japan_ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____Giophantus_____, 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____Giophantus_; **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, 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: Kaji Nuida

Title: Associate Professor

Date: April 4, 2018

Place: Tokyo, Japan

2.D.1 Statement by Each Submitter

I,_____Shinya Okumura_____, of_____1-2, Yamadaoka, Suita, Osaka, Japan_, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as____Giophantus_____, 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____Giophantus_; **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, 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: Shinya Okumura

Title: Assistant Professor

Date: April 2, 2018

Place: Suita, Japan

2.D.1 Statement by Each Submitter

I,_____Hideo Shimizu_____, of_____1, Komukai-Toshiba-cho, Kawasaki, Kanagawa, Japan_____, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as _____Giophantus_____, 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____Giophantus_; **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, 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: *Hideo Shimizu*

Title: *chief research Scientist*

Date: *Mar 29. 2018*

Place: *Kawasaki Japan*

2.D.1 Statement by Each Submitter

I,_____Tsuyoshi Takagi_____, of_ 7-3-1, Hongo, Bunkyo-ku, Tokyo, Japan_____,
do hereby declare that the cryptosystem, reference implementation, or optimized
implementations that I have submitted, known as_Giophantus___, 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____Giophantus_;
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_____Giophantus_____, 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,
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: *Tsuyoshi Takagi*

Title: *Professor*

Date: *March 29, 2018*

Place: *Tokyo, Japan*

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

The following must also be included:

I,_____Hideo Shimizu_____, 1, Komukai-Toshiba-cho, Kawasaki, Kanagawa, 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: Hideo Shimizu

Title: Chief research scientist

Date: Mar 29 2018

Place: Kawasaki Japan