l,	_Koichiro Akiyama	of	1, Komul	kai-Toshiba-cho,
Kawas	saki, Kanagawa, Japa nentation, or optimiz	ın, do hereby	declare that the	cryptosystem, reference
·				r if submitted jointly
with o	thers, is the original			, ,
l furth	er declare that (chec	k one):		
V	claim which may co	over the cryptosyste entations that I have	em, reference im <sub>l</sub> e submitted, kno	atent application with a plementation, or wn asGiophantus ;
	reference in submitted, i the followin □ I do hereby pending U.S of my subm	known as ng U.S. and/or forei declare that, to the 5. and/or foreign pa	optimized implenGiophantus gn patents:no best of my know tent applications reference imple	nentations that I have , may be covered by

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the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use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

,Yasuhir	ro Goto	, of	1-2 Hachiman-ch	io, Hakodate,
Hokkaido, Jap	an	, do hereby	declare that the cryptos	ystem, reference
•	· ·	-	s that I have submitted,	
Giopha	ntus	is my own	original work, or if subn	nitted jointly
with others, is	the original work o	of the joint sub	omitters.	
I further decla	re that (check one).			
jurtiler accia	re that (eneck one).			
claim optim	which may cover th	he cryptosyste ons that I have	any patent or patent ap m, reference implement submitted, known as ):	ation, or
	reference implem submitted, knowr , m	nentation, or on as nay be covered	he practice of the crypto ptimized implementatio _(print name of cryptos d by the following U.S. a umerate or state "none	ns that I have system) nd/or foreign
	pending U.S. and, of my submitted o	/or foreign pa cryptosystem,	best of my knowledge, t tent applications may co reference implementati be and enumerate or sta	over the practice ion or optimized

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

Signed:

Title:

Professor

Date:

March 30, 2018

Place:

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

l,Go	ichiro Hanaoka	of	2-3-26, Aomi, Kot	to-ku, Tokyo,				
Japan_, de	o hereby declare tha	nt the cryptosyste	em, reference implemente	ation, or				
optimized	implementations t	hat I have submi	tted, known as					
Giophantus, is my own original work, or if submitted jointly								
with othe	rs, is the original wo	rk of the joint su	bmitters.					
l further a	leclare that (check o	ne):						
cl o <sub>l</sub>	aim which may cove	er the cryptosyste ations that I have	d any patent or patent ap em, reference implement e submitted, known as 1):	ation, or				
	_		the practice of the crypto optimized implementation	•				
	submitted, kno	own as	(print name of cryptos	ystem)				
			d by the following U.S. ar					
	patents:	_(describe and er _;	numerate or state "none"	' if applicable)				
	pending U.S. a of my submitt	and/or foreign pa ed cryptosystem,	e best of my knowledge, t itent applications may co reference implementation be and enumerate or sta	ver the practice on or optimized				

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

Goich! to Hanaoke Signed:

Leader, Advanced Cryptosystems Research Group, AIST Title:

Apr. 2, 2018 Date:

Tokyo, Japan Place:

# 2.D.1 Statement by Each Submitter \_\_\_Yasuhiko Ikematsu\_\_\_\_\_\_, of<u>\_\_7-3-</u>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 <u>Giophantus</u>, may be covered by the following U.S. and/or foreign patents: <u>none</u> $\square$ 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

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).

implementations: none

of my submitted cryptosystem, reference implementation or optimized

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: Yashhiko Ikematsh

Title: project Veseakher

Date: April 2, 2018

Place: Tokyo, Japan

,Koji Nu	ida	, of	7-3-1 Hongo, Bui	nkyo-ku, Tokyo,
			reference implement	
optimized imp	olementations that I	have submitte	d, known as	
Giopha	ntus	j is my own or	iginal work, or if subn	nitted jointly
with others, is	the original work of	the joint subm	itters.	
further decla	re that (check one):			
			ny patent or patent ap	
	·		reference implement	
	The state of the s		ıbmitted, known as	Giophantus ;
OR (ch	heck one or both of t	he following):		
	to the best of my k	nowledge, the	practice of the crypto	system,
			imized implementatio	
	submitted, known	as(	print name of cryptos	ystem)
	, ma	ly be covered b	y the following U.S. a	nd/or foreign
	patents:(des	cribe and enun	nerate or state "none	" if applicable)
	I do hereby declare	that, to the be	est of my knowledge, t	the following
	pending U.S. and/o	or foreign pater	nt applications may co	over the practice
	of my submitted cr	yptosystem, re	ference implementati	on or optimized
	implementations:_	(describe	and enumerate or sta	ite "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

Signed: Kaji Nuida

Title: Associate Professor

Date: April 4, 2018

Place: Tokyo, Japan

2.D.1	Statement by Each S	ubmitter	
1,	Shinya Okumura	, of	1-2, Yamadaoka, Suita, Osaka,
Japan implei	_, do hereby declare the mentations that I have	nat the cryptosystem, i submitted, known as	reference implementation, or optimized Giophantus, is
my ov submi		submitted jointly with	others, is the original work of the joint
I furth	er declare that (check	one):	
Z	claim which may co	ver the cryptosystem, i at I have submitted, kr	y patent or patent application with a reference implementation, or optimized nown asGiophantus; <b>OR</b> (check one
	implementa	tion, or optimized imp	practice of the cryptosystem, reference lementations that I have submitted,
	following U.		tosystem), may be covered by the nts:(describe and enumerate or
	☐ I do hereby o pending U.S. my submitte	declare that, to the best and/or foreign patent ad cryptosystem, referent tions:(describe o	st of my knowledge, the following t applications may cover the practice of ence implementation or optimized and enumerate or state "none" if

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

signed: Shinya Okumura

Title: Assistant Professor

Date: April 2, 2018

Place: Suita, Japan

I,Hideo S	Shimizu	of	1, Komukai-Toshiba-	cho,
Kawasaki, Kar implementati	nagawa, Japan on, or optimized ir	, do hereb mplementatio	y declare that the cryptosyste ons that I have submitted, kno n original work, or if submitte	em, reference own as
	the original work			,
I further decla	re that (chèck one	):		
claim optim	which may cover t	the cryptosyst ons that I hav	d any patent or patent applic em, reference implementatio re submitted, known asG g):	on, or
	reference implen submitted, know , r patents:(d ; I do hereby decla pending U.S. and of my submitted	mentation, or on as may be covered and each are that, to the cryptosystem	the practice of the cryptosyste optimized implementations to(print name of cryptosystem of the following U.S. and/ornumerate or state "none" if or a best of my knowledge, the patent applications may cover on, reference implementation or state "	hat I have em) or foreign applicable) following the practice or optimized

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

Signed: Kideo Shimiya

Title: chief research Scientist

Date: Mar 29. 2018

Place: Kawasaki Japan

# 2.D.1 Statement by Each Submitter \_\_Tsuyoshi Takagi\_\_\_\_\_\_\_, of<u>7-3-</u>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 <u>Giophantus</u>, may be covered by the following U.S. and/or foreign patents: <u>none</u> ☐ 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

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).

implementations: <u>none</u>

of my submitted cryptosystem, reference implementation or optimized

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.

Tokyo, Japan Signed:

Title:

Date:

Place:

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

The fol	lowing	must	also	be	incl	uded	:

I, <u>Hideo Shimizu</u>, 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: Hider Shimiza

Title: Chief research scientist

Date: Mar 29 2018

Place: Kanasaki Japan