Statement by Each Submitter

D : 1 T D 1: (5 86) 5 M - (W/C) (1 - 1 60/07-7063
I, Daniel J. Bernstein, of C5,851 S. Morgan (MC 152), Chicago, IL 60607-7053, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Post-Quantum KSA, 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 reference implementation, or optimized implementations that I have 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, 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: D. J. Benston
Title: Research Professor
Date: 14 March 2018
Place: Eindhoven

Statement by Each Submitter

nereby declare that the cryptosystem, reference implementation, or optimized implementations that I has submitted, known as Post - Quantum RSA, is my own original work, or if submitted join with others, is the original work of the joint submitters. I further declare that (check one):	vue.
■ I do not hold and do not intend to hold any patent or patent application with a claim whimay cover the cryptosystem, reference implementation, or optimized implementations that I has submitted, known as Portocover ISA OR (check one or both of the following) □ to the best of my knowledge, the practice of the cryptosystem, reference implementation, optimized implementations that I have submitted, known as	or be /or nce
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public preview and will be evaluated by NIST, and that it might not be selected for standardization by NIST further acknowledge that I will not receive financial or other compensation from the U.S. Government my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and pate applications which may cover my cryptosystem, reference implementation or optimized implementation I also acknowledge and agree that the U.S. Government may, during the public review and the evaluate process, and, if my submitted cryptosystem is selected for standardization, during the lifetime of standard, modify my submitted cryptosystem's specifications (e.g., to protect against a newly discovery vulnerability).	for ent ns. ion the
I acknowledge that NIST will announce any selected $cryptosystem(s)$ and proceed to publish the dr $standards$ for public comment.	raft
I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any pat or patent application identified to cover the practice of my cryptosystem, reference implementation optimized implementations and the right to use such implementations for the purposes of the public revealed evaluation process.	, 01
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my creatosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem, removed from consideration for standardization or withdrawn from consideration by all submitter(s) cowner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.L including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.) is and D.3,
Signed:	
Title: Assistant Professor	
Date: 3-16-2018	Tes:
Place: Philadelphia PA	

Statement by Each Submitter
I, Paul S. Lou of Move 102, 220 S. 33 al Street, Philadelphia, M. 19104, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Post - Quantum RSA, 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 Post - Quantum RSH 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, 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: Jan
Title: Undergraduate Student
Title: Undergraduate Student Date: Place:
Philadelphia, PA 19104, USA

Statem

Statement by Each Submitter
I, Luke Valenta, of Moor 12,220 5. 32d Street Philocolphia, 14 19104, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Post-Quantum RSA, 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 asOR (check one or both of the following): \[\begin{align*} & 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, 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: Yn 2 X Title: PhD Student
Date: 14 March 2018
Place: Philadolphica

The following must also be included:				
I, Daniel J. Bernstein owner or authorized representative of	CS, 851 S. Mai	gom (M/C152), Chic	cago, IL 6060	7-7053, am the
owner or authorized representative of	the owner	Daniel J. Benestein	of th	e submitted ref-
erence implementation and optimized	$l\ implementation$	s and hereby grant	the U.S. Gover	nment and any
interested party the right to reproduce	e, prepare derivati	ive works based upor	n, distribute con	oies of, and dis-
play such implementations for the pu	irposes of the pos	t-quantum algorithm	n public review	and evaluation
process, and implementation if the co	orresponding cryp	otosystem is selected	d for standardi	zation and as a
standard, notwithstanding that the im	anlementations m	an be congrighted of	r convriattable	

Signed: D.J. Geunten
Title: Research Professor
Date: 14 March 2018
Place: Eindhoven

The following must also be included:
I, Josha Fried, of 32/1958, 4, 32 6978B, Cambridge MA, am the
exerce implementation and ontimized implementations and hereby grant the U.S. Government and any
interested narty the right to reproduce, prepare derivative works based upon, distribute copies of, and ais-
play 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: John Told
Title: PhD Styles it
Date: 4/2/18
Place: Cambridge, MA

The following must also be included:
I, Nacha Hening 3330 Uclinit I. Philipple PA 15109, 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:
Title: Assistant Professor
Date: 3-16-2018
Place: Philadelphia PA

The following must also be included:	Steet, Philadelphia, 174 19104
The following must also be included: I, Paul S. Lou, Mour 162, 220 S. 33 d.S.	, am the
some an authorized representative of the owner	Of the businesses is
erence implementation and optimized implementations and hereby grant interested party the right to reproduce, prepare derivative works based upplay such implementations for the purposes of the post-quantum algorith process, and implementation if the corresponding cryptosystem is select standard, notwithstanding that the implementations may be copyrighted	on, assirtante copies of, and assirtante copies of a
Signed:	
Title: Under graduate Student	
Date: 15 March 2018	
Philadelphia, PA 19104, USA	

The following must als	o be included:	in the Author Source
1. Luke Vale	ta , More (02, 220 s.	33rd Street, Philadephia, PA 19104, am the
owner or authorized re	presentative of the owner	of the submitted ref
amon or amontom entation	and antimized illineralementations and	L HELEGY WILLIAM CO. C. C.
interested narty the ric	ht to reproduce, prepare derivative wo	orks basea upon, distribute copies of, and and
mlass auch immlementat	ions for the nurposes of the post-quar	intum algorithm public review and evaluation
process and implemen	station if the corresponding cryptosys	stem is selected for standardization and as
standard, notwithstane	ling that the implementations may be	e copyrighted or copyrightable.
Signed: Yr Vw	L	
)	

Date: 14 March 2018
Place: Philadelphia