SECURE RF

Securing the Internet of Things®

January 22, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Post-Quantum Cryptography Standardization Proposal
Section 2.D.1: Statement by Each Submitter

Dear Madam or Sir:

I, ***Iris Anshel, Ph.D., Chief Scientist, SecureRF Corporation**, of **100 Beard Sawmill Road, Shelton, Connecticut 06484***, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***The Walnut Digital Signature Algorithm ("WalnutDSA")***, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare:

□ To the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***WalnutDSA*** may be covered by the following U.S. and/or foreign patents:

7,649,999	***Method and Apparatus for Establishing Key Agreement Protocol***
9,071,427	***Method and Apparatus for Establishing Key Agreement Protocol***

□ 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:

Patent Pending *(Application Filed: September 20, 2016 with priority to provisional patent application dated September 22, 2015)*	***Signature Generation and Verification System***

Patent Pending *(Continuation-in-Part Application Filed: November 17, 2017, to U.S. Application filed September 20, 2016 with priority to provisional patent application dated September 22, 2015)*	***Signature Generation and Verification System, Application, Continuation-in-Part***

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 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), 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 (Statement by Each Submitter), 2.D.2 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Respectfully submitted,

By: Iris Anshel
Print Name: *Iris Anshel*
Title: *Chief Scientist, SecureRF Corporation*
Date: January 22, 2018
Place: Shelton, CT USA

SECURE RF

Securing the Internet of Things®

January 22, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: *Post-Quantum Cryptography Standardization Proposal*
Section 2.D.1: Statement by Each Submitter

Dear Madam or Sir:

I, ***Derek Atkins, Chief Technology Officer, SecureRF Corporation**, of **100 Beard Sawmill Road, Shelton, Connecticut 06484***, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***The Walnut Digital Signature Algorithm ("WalnutDSA")**,* is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare:

□ To the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***WalnutDSA**, a component of which* may be covered by the following U.S. and/or foreign patents:

7,649,999 ***Method and Apparatus for Establishing Key Agreement Protocol***

9,071,427 ***Method and Apparatus for Establishing Key Agreement Protocol***

□ 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:

Patent Pending *(Application Filed: September 20, 2016 with priority to provisional patent application dated September 22, 2015)*	***Signature Generation and Verification System***

Patent Pending *(Continuation-in-Part Application Filed: November 17, 2017, to U.S. Application filed September 20, 2016 with priority to provisional patent application dated September 22, 2015)*	***Signature Generation and Verification System, Application, Continuation-in-Part***

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 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), 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 (Statement by Each Submitter), 2.D.2 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Respectfully submitted,

By:	
Print Name:	*Derek Atkins*
Title:	*Chief Technology Officer, SecureRF Corporation*
Date:	January 22, 2018
Place:	Shelton, CT USA

SECURE RF

Securing the Internet of Things®

January 22, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Post-Quantum Cryptography Standardization Proposal
Section 2.D.1: Statement by Each Submitter

Dear Madam or Sir:

I, ***Dorian Goldfeld, Ph.D., Founder & Advisor, SecureRF Corporation**, of **100 Beard Sawmill Road, Shelton, Connecticut 06484***, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***The Walnut Digital Signature Algorithm ("WalnutDSA")***, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare:

□ To the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***WalnutDSA*** may be covered by the following U.S. and/or foreign patents:

7,649,999 ***Method and Apparatus for Establishing Key Agreement Protocol***

9,071,427 ***Method and Apparatus for Establishing Key Agreement Protocol***

□ 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:

Patent Pending *(Application Filed: September 20, 2016 with priority to provisional patent application dated September 22, 2015)*	***Signature Generation and Verification System***

Patent Pending
(Continuation-in-Part Application Filed: November 17, 2017, to U.S. Application filed September 20, 2016 with priority to provisional patent application dated September 22, 2015)

Signature Generation and Verification System, Application, Continuation-in-Part

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 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), 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 (Statement by Each Submitter), 2.D.2 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Respectfully submitted,

By:
Print Name: *Dorian Goldfeld, Ph.D.*
Title: *Chief Technology Officer, SecureRF Corporation*
Date: January 22, 2018
Place: Shelton, CT USA

SECURE RF

Securing the Internet of Things®

January 22, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: Post-Quantum Cryptography Standardization Proposal
Section 2.D.1: Statement by Each Submitter

Dear Madam or Sir:

I, ***Paul Edward Gunnells, Ph.D., Advisor, SecureRF Corporation**, of **100 Beard Sawmill Road, Shelton, Connecticut 06484***, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***The Walnut Digital Signature Algorithm ("WalnutDSA")***, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare:

□ To the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ***WalnutDSA*** may be covered by the following U.S. and/or foreign patents:

7,649,999 ***Method and Apparatus for Establishing Key Agreement Protocol***

9,071,427 ***Method and Apparatus for Establishing Key Agreement Protocol***

□ 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:

Patent Pending ***Signature Generation and Verification System***
(Application Filed: September 20, 2016 with priority to provisional patent application dated September 22, 2015)

Patent Pending *(Continuation-in-Part Application Filed: November 17, 2017, to U.S. Application filed September 20, 2016 with priority to provisional patent application dated September 22, 2015)*	***Signature Generation and Verification System, Application, Continuation-in-Part***

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 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), 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 (Statement by Each Submitter), 2.D.2 (Statement by Patent (and Patent Application) Owner(s)) and 2.D.3 (Statement by Reference/Optimized Implementations' Owner(s)), including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Respectfully submitted,

By: ____________________
Print Name: *Paul Edward Gunnells*
Title: *Advisor, SecureRF Corporation*
Date: January 22, 2018
Place: Shelton, CT

SECURE RF

Securing the Internet of Things®

January 22, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

RE: *Post-Quantum Cryptography Standardization Proposal*
Section 2.D.2: Statement by Patent (and Patent Application) Owner(s)

Dear Madam or Sir:

I, ***SecureRF Corporation***, of ***100 Beard Sawmill Road, Shelton, Connecticut 06484***, am the owner or authorized representative of the owner of commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as ***The Walnut Digital Signature Algorithm ("WalnutDSA")*** is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard:

- 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, non-transferrable, 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.

Respectfully submitted,

By:

Print Name: *Derek Atkins*

Title: *Chief Technology Officer, SecureRF Corporation*

Date: January 22, 2018

Place: Shelton, CT USA

SECURE RF

Securing the Internet of Things®

January 22, 2018

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, Maryland 20899

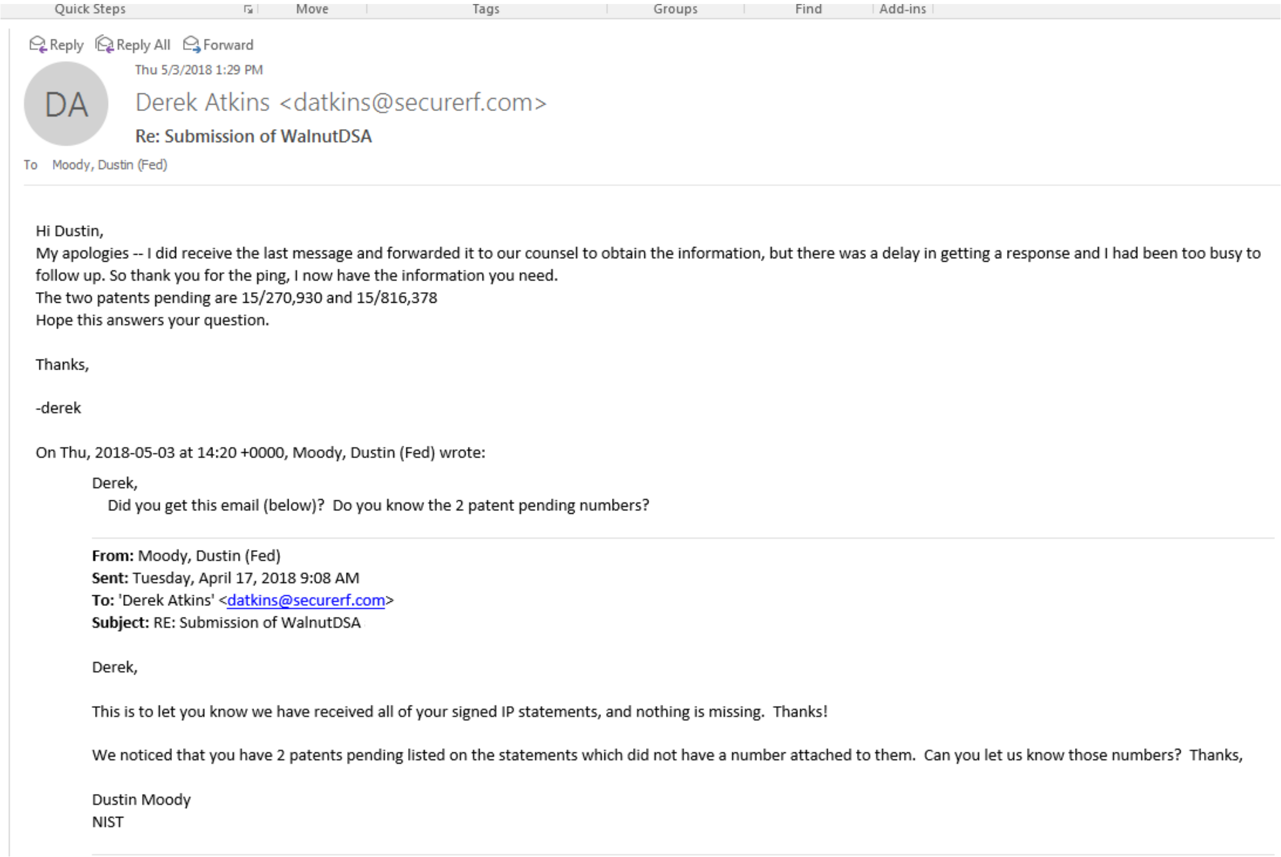
RE: *Post-Quantum Cryptography Standardization Proposal*
Section 2.D.3: Statement by Reference/Optimized Implementations' Owner(s)

Dear Madam or Sir:

I, ***SecureRF Corporation**, of **100 Beard Sawmill Road, Shelton, Connecticut 06484***, am the owner or authorized representative of the owner of the submitted reference implementation and optimized implementations of ***The Walnut Digital Signature Algorithm ("WalnutDSA")*** 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.

Respectfully submitted,

By:
Print Name: *Derek Atkins*
Title: *Chief Technology Officer, SecureRF Corporation*
Date: January 22, 2018
Place: Shelton, CT USA



Thu 5/3/2018 1:29 PM

Derek Atkins <datkins@securerf.com>

Re: Submission of WalnutDSA

To Moody, Dustin (Fed)

Hi Dustin,
My apologies -- I did receive the last message and forwarded it to our counsel to obtain the information, but there was a delay in getting a response and I had been too busy to follow up. So thank you for the ping, I now have the information you need.
The two patents pending are 15/270,930 and 15/816,378
Hope this answers your question.

Thanks,

-derek

On Thu, 2018-05-03 at 14:20 +0000, Moody, Dustin (Fed) wrote:

> Derek,
> Did you get this email (below)? Do you know the 2 patent pending numbers?
>
> **From:** Moody, Dustin (Fed)
> **Sent:** Tuesday, April 17, 2018 9:08 AM
> **To:** 'Derek Atkins' <datkins@securerf.com>
> **Subject:** RE: Submission of WalnutDSA
>
> Derek,
>
> This is to let you know we have received all of your signed IP statements, and nothing is missing. Thanks!
>
> We noticed that you have 2 patents pending listed on the statements which did not have a number attached to them. Can you let us know those numbers? Thanks,
>
> Dustin Moody
> NIST