NTS-KEM

Principal submitter:

This submission is from the following team, listed in alphabetical order:

- Martin Albrecht, martin.albrecht@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Carlos Cid, carlos.cid@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Kenneth G. Paterson, kenny.paterson@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Cen Jung Tjhai, cjt@post-quantum.com, PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom, +44 203 713 7388
- Martin Tomlinson, mt@post-quantum.com, PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom, +44 203 713 7388

Auxiliary submitters: There are no auxiliary submitters.

Inventors/developers: The inventors/developers of this submission are the same as the principal submitter. Relevant prior work is credited below where appropriate.

Owner: PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom.

Signature:

Martin Albrecht	Carlos Cid	Kenneth G. Paterson	Cen Jung Tjhai	Martin Tomlinson

MAUCHER
JENKINS

Our Case: HEW/AL/ J102467GB/J102467US
Your Ref: Crypto3

26 Caxton Street
London SW1H 0RJ
T: +44(0) 20 7931 7141
F: +44(0) 20 7222 4660
info@maucherjenkins.com
www.maucherjenkins.com

27 April 2018

PQ Solutions Limited
50 Liverpool Street
London
EC2M 7PR
United Kingdom

BY EMAIL
To: mt@post-quantum.com; ac@post-quantum.com.

Dear Andersen, Martin,

UK Patent No. GB2532242
Martin Tomlinson, Cen Jung Tjhai
and
United States Patent Application No. 14/596098
PQ Solutions Limited
Public Key Cryptosystem using Error Correcting Codes

We confirm receipt of your instructions of 26 April 2018 to abandon the above-referenced GB patent and US patent application.

We will forward official confirmation of abandonment from the respective patent office to you once received.

Yours faithfully

Alvin Lam
Maucher Jenkins

London | Farnham | Cambridge | Edinburgh | Munich | Freiburg | Basel | Beijing
European Patent Attorneys | Chartered Patent Attorneys | German Patent Attorneys | Chartered Trade Mark Attorneys | Attorneys-at-Law | IP Litigators
Partners: James Cross, Tim Pendered, Hugh Dunlop, Reuben Jacob, Felix Rummler, Holly Whitlock, Philip Treeby, Angela Fox,
Katie Cameron, Cornelius Mertzlufft-Paufler, Handong Ran, Kei Enomoto, Alvin Lam, Kana Enomoto, Michael Nielen
Consultants: Henrich Börjes-Pestalozza, David Musker, Alec Clelland
Maucher Jenkins® is the joint trading name of RGC Jenkins & Co in the UK (regulated by IPReg) and Maucher Jenkins Patentanwälte & Rechtsanwälte in Germany.

NTS-KEM

Principal submitter:

This submission is from the following team, listed in alphabetical order:

- Martin Albrecht, martin.albrecht@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Carlos Cid, carlos.cid@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Kenneth G. Paterson, kenny.paterson@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Cen Jung Tjhai, cjt@post-quantum.com, PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom, +44 203 713 7388
- Martin Tomlinson, mt@post-quantum.com, PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom, +44 203 713 7388

Auxiliary submitters: There are no auxiliary submitters.

Inventors/developers: The inventors/developers of this submission are the same as the principal submitter. Relevant prior work is credited below where appropriate.

Owner: PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom.

Signature:

Martin Albrecht	Carlos Cid	Kenneth G. Paterson	Cen Jung Tjhai	Martin Tomlinson

NTS-KEM

Principal submitter:

This submission is from the following team, listed in alphabetical order:

- Martin Albrecht, martin.albrecht@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Carlos Cid, carlos.cid@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Kenneth G. Paterson, kenny.paterson@rhul.ac.uk, Information Security Group & Institute for Cyber Security Innovation, Royal Holloway University of London, Egham, Surrey, TW20 0EX, United Kingdom, +44 (0)1784 434455
- Cen Jung Tjhai, cjt@post-quantum.com, PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom, +44 203 713 7388
- Martin Tomlinson, mt@post-quantum.com, PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom, +44 203 713 7388

Auxiliary submitters: There are no auxiliary submitters.

Inventors/developers: The inventors/developers of this submission are the same as the principal submitter. Relevant prior work is credited below where appropriate.

Owner: PQ Solutions Ltd, 50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom.

Signature:

				M. Tomlinson
Martin Albrecht	Carlos Cid	Kenneth G. Paterson	Cen Jung Tjhai	Martin Tomlinson

I, **Martin Albrecht** *of* **Royal Holloway, University of London** *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *may be covered by the following U.S. and/or foreign patents:* **GB2532242 Public Key Cryptosystem using Error Correcting Codes**
- *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:* **US20150163060 Methods, systems and apparatus for public key encryption using error correcting codes**

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: **Lecturer Information Security Group**

Date: **6 November 2017**

Place: **Royal Holloway University of London, Egham, Surrey, TW20 0EX, UK**

I, **Carlos Cid** *of* **Royal Holloway, University of London** *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *may be covered by the following U.S. and/or foreign patents:* **GB2532242 Public Key Cryptosystem using Error Correcting Codes**
- *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:* **US20150163060 Methods, systems and apparatus for public key encryption using error correcting codes**

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: Carlos Cid

Title: **Professor Information Security Group**

Date: **6 November 2017**

Place: **Royal Holloway University of London, Egham, Surrey, TW20 0EX, UK**

I, **Kenneth G. Paterson** *of* **Royal Holloway, University of London** *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *may be covered by the following U.S. and/or foreign patents:* **GB2532242 Public Key Cryptosystem using Error Correcting Codes**
- *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:* **US20150163060 Methods, systems and apparatus for public key encryption using error correcting codes**

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 Information Security Group**

Date: **6 November 2017**

Place: **Royal Holloway University of London, Egham, Surrey, TW20 0EX, UK**

I, **Cen Jung Tjhai** *of* **PQ Solutions Ltd** *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *may be covered by the following U.S. and/or foreign patents:* **GB2532242 Public Key Cryptosystem using Error Correcting Codes**
- *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:* **US20150163060 Methods, systems and apparatus for public key encryption using error correcting codes**

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: **Chief Architect**

Date: **6 November 2017**

Place: **50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom**

I, **Martin Tomlinson** *of* **PQ Solutions Ltd** *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *is my own original work, or if submitted jointly with others, is the original work of the joint submitters. I further declare that*

- *to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **NTS-KEM** *may be covered by the following U.S. and/or foreign patents:* **GB2532242 Public Key Cryptosystem using Error Correcting Codes**
- *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:* **US20150163060 Methods, systems and apparatus for public key encryption using error correcting codes**

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: M. T

Title: **CSO**

Date: **6 November 2017**

Place: **50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom**

G.2 Statement by Patent (and Patent Application) Owner(s)

I, **Andersen Cheng** *of* **PQ Solutions Ltd** *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):*
GB2532242 Public Key Cryptosystem using Error Correcting Codes
US20150163060 Methods, systems and apparatus for public key encryption using error correcting codes
and do hereby commit and agree to grant to any interested party on a worldwide basis, if the cryptosystem known as **NTS-KEM** *is selected for standardization, in consideration of its evaluation and selection by NIST, a non-exclusive license for the purpose of implementing the standard:*

- *without compensation and 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: **CEO. PQ Solutions Ltd**

Date: **6 November 2017**

Place: **50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom**

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

The following must also be included:

I, **Andersen Cheng** *am the owner or authorized representative of the owner* **PQ Solutions Ltd** *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: **CEO. PQ Solutions Ltd**

Date: **6 November 2017**

Place: **50 Liverpool Street, 5th floor, London, EC2M 7PR, United Kingdom**