

Name of the proposed cryptosystem:

Mirath

Principal submitter:

Gora Adj, Technology Innovation Institute, UAE
Nicolas Aragon, Naquidis Center, Talence
Stefano Barbero, Politecnico di Torino
Magali Bardet, University of Rouen and INRIA
Emanuele Bellini, Technology Innovation Institute, UAE
Loïc Bidoux, Technology Innovation Institute, UAE
Jesús-Javier Chi-Domínguez, Technology Innovation Institute, UAE
Victor Dyzeryn, University of Limoges
Andre Esser, Technology Innovation Institute, UAE
Thibault Feneuil, CryptoExperts
Philippe Gaborit, University of Limoges
Romaric Neveu, University of Limoges
Matthieu Rivain, CryptoExperts
Luis Rivera-Zamarripa, Technology Innovation Institute, UAE
Carlo Sanna, Politecnico di Torino
Jean-Pierre Tillich, INRIA
Javier Verbel, Technology Innovation Institute, UAE
Floyd Zweyding, Technology Innovation Institute, UAE

Inventors:

Same as submitters

Owners:

Same as submitters

E-mail address:

team@pqc-mirath.org

Postal address:

Mirath Consortium
XLIM - DMI
Université de Limoges
123 Avenue Albert Thomas
87 060 Limoges CEDEX
FRANCE

Signed: Gora Adj

Title: Dr.

Date: 31/01/2025

Place: Abu Dhabi, United Arab Emirates

A handwritten signature in black ink, consisting of a series of loops and a vertical stroke, positioned to the right of the text.

Signed:
Title: PhD
Date: January 15, 2025
Place: Limoges



Signed:

Stefano Portero


Title: Ph. D.

Date: January 15, 2025

Place: Torino, Italy

Signed: Magali Bardet
Title: Maître de conférences
Date: 17/01/2025
Place: Rouen, France

A handwritten signature in black ink, appearing to read 'Magali Bardet', with a horizontal line underneath.

Signed: 

Title: Dr. Emanuele Bellini

Date: 15/01/2025

Place: Abu Dhabi

Signed: Loïc Bidoux
Title: Dr
Date: 15/01/2025
Place: Abu Dhabi

A handwritten signature in black ink, consisting of a stylized capital 'B' with a horizontal line through it, followed by a long horizontal stroke.

Signed: Jesús Javier Chi Domínguez
Title: Dr.
Date: 15/01/2025
Place: Abu Dhabi, UAE

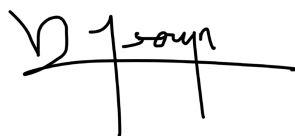
A handwritten signature in blue ink, appearing to read 'Jesús Chi Domínguez', written in a cursive style.


Signed: Victor DYSERYN

Title: Dr.

Date: January 15, 2025

Place: Palaiseau

A handwritten signature in black ink, appearing to read "V. Dyseryn", written over a horizontal line.

Signed: 

Title: PhD

Date: 15th January 2025

Place: Abu Dhabi

Signed: Thibauld Feneuil

Title: Dr.

Date: 15/01/2025

Place: Paris, France

A handwritten signature in black ink. The name 'Thibauld' is written in a cursive style, with a large 'T' and 'd'. Below it, the name 'FENEUIL' is written in a straight, uppercase font. The entire signature is enclosed within a simple, hand-drawn rectangular border.

Signed: philippe gaborit
Title: Professor
Date: January 15 2025
Place: Limoges, France

P. Gaborit.

A handwritten signature in blue ink, appearing to be 'P. Gaborit', with a long, sweeping underline.

Signed: Romaric NEVEU

Title: Mr.

Date: January 15 2025

Place: Limoges

A handwritten signature in black ink, appearing to read 'R Neveu'. The signature is stylized, with a large, bold 'R' and the name 'Neveu' written in a cursive script.

Signed: Matthieu Rivain

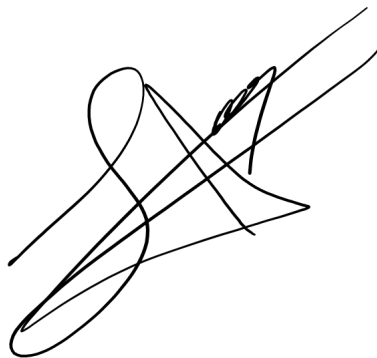
Title: Dr.

Date: 20/01/2025


Place: Paris

A handwritten signature in black ink, consisting of a stylized 'M' and 'R' intertwined.

Signed: LuisAlberto Rivera Zamarripa
Title: Dr.
Date: 24/01/2025
Place: Abu Dhabi, UAE

A handwritten signature in black ink, consisting of several overlapping loops and a final horizontal stroke, positioned to the right of the text.

Signed:

A handwritten signature in black ink, reading "Carlo Lamma". The script is cursive and fluid, with the first name "Carlo" and the last name "Lamma" clearly distinguishable.

Title: PhD

Date: January 15, 2025

Place: Torino, Italy

Signed: Jean-Pierre Tillich
Title: Dr.
Date: February 3rd 2025
Place: Paris

A handwritten signature in black ink, appearing to read 'J. P. Tillich', with a large, sweeping flourish extending from the bottom left.

Signed:

Javier Verbel H.

Title: Dr

Date: January 15th, 2025

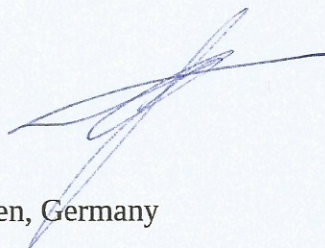
Place: Abu Dhabi, United Arab Emirates

Signed:

Title:

Date: 31.01.25

Place: Hattingen, Germany

A handwritten signature in blue ink, consisting of several overlapping, fluid strokes that form a stylized, abstract shape.

I, **Gora Adj**, of **Technology Innovation Institute, P.O. Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Gora Adj

Title: Dr.

Date: 31/01/2025

Place: Abu Dhabi, United Arab Emirates



IP Statement of Nicolas Aragon

I, Nicolas Aragon, of University of Limoges, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**; 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 **Mirath**, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state “none” if applicable)_____ ;
- ☐ 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: PhD

Date: November 1st, 2024

Place: Limoges, France

IP Statement of Stefano Barbero

I, Stefano Barbero, of Politecnico di Torino, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**; 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 **Mirath**, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state “none” if applicable)_____ ;
- ☐ 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: PhD

Date: November 1st, 2024

Place: Torino, Italy

I, **Magali Bardet**, of **LITIS, Université de Rouen Normandie, avenue de l'Université, 76800 Saint-Étienne-du-Rouvray**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Magali BARDET
Title: Maître de conférences
Date: 17/01/2025
Place: Rouen, France



I, **Emanuele Bellini**, of **Technology Innovation Institute, Abu Dhabi, UAE**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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):

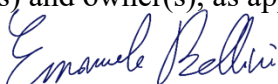
- ☒ I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: 

Title: Dr. Emanuele Bellini

Date: 15/01/2025

Place: Abu Dhabi

I, **Loïc Bidoux**, of **Technology Innovation Institute, P.O.Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;

☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Loïc Bidoux

Title: Dr

Date: 15/01/2025

Place: Abu Dhabi

A handwritten signature in black ink, consisting of a stylized 'B' followed by a horizontal line and a small flourish.

I, **Jesús Javier Chi Domínguez**, of **Technology Innovation Institute, P.O. Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Jesús Javier Chi Domínguez
Title: Dr.
Date: 15/01/2025
Place: Abu Dhabi, UAE



I, **Victor DYSERYN**, of **Télécom Paris, 19, place Marguerite Perey, 91120 Palaiseau, FRANCE**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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.

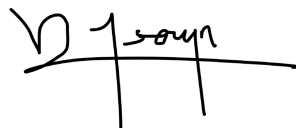
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and 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: Victor DYSERYN

Title: Dr.

Date: January 15, 2025

Place: Palaiseau

A handwritten signature in black ink, appearing to read 'V. Dyseryn', with a horizontal line extending to the right.

IP Statement of Andre Esser

I, Andre Esser, of Technology Innovation Institute, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**; 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 **Mirath**, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state “none” if applicable)_____ ;
- ☐ 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: PhD

Date: November 1st, 2024

Place: Abu Dhabi, UAE

I, **Thibault Feneuil**, of **CryptoExperts, 41 Boulevard des Capucines, 75002 Paris, France**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Thibault Feneuil

Title: Dr.

Date: 15/01/2025

Place: Paris, France

A handwritten signature in black ink that reads "Thibault FENEUIL". The signature is stylized, with a long horizontal stroke at the bottom and a checkmark-like flourish on the left side.

I, **philippe gaborit**, of University of Limoges, 123 avenue albert thomas, 87000 Limoges, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: philippe gaborit
Title: Professor
Date: January 15 2025
Place: Limoges , France

P. Gaborit.



I, **Romaric NEVEU**, of **XLIM, 123 Av. Albert Thomas, 87000 Limoges, France**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Romaric NEVEU

Title: Mr.

Date: January 15 2025

Place: Limoges



I, **Matthieu Rivain**, of **CryptoExperts, 41 boulevard des Capucines, 75002 Paris**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Matthieu Rivain

Title: Dr.

Date: 20/01/2025

Place: Paris



I, **Luis Alberto Rivera Zamarripa**, of **Technology Innovation Institute, P.O.Box: 9639, Yas Island, Abu Dhabi, United Arab Emirate**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;
- ☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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.

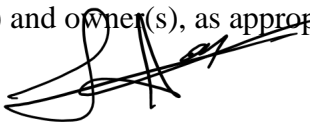
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and 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:

Title: Dr.

Date: 24/01/2025

Place: Abu Dhabi



IP Statement of Carlo Sanna

I, Carlo Sanna, of Politecnico di Torino, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**; 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 **Mirath**, may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state “none” if applicable)_____ ;
- ☐ 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: PhD

Date: November 1st, 2024

Place: Torino, Italy

I, **Jean-Pierre TILLICH**, from **Inria, 48 rue Barrault Paris 75012, FRANCE**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;



to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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: Jean-Pierre Tillich

Title: Dr.

Date: February 3rd 2025

Place: Paris



I, **Javier Alfonso Verbel Herrera Technology Innovation Institute, P.O.Box:9639, Yas Island, Abu Dhabi, United Arab Emirates**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;

☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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.

I, **Floyd Zweydinger**, of **Technology Innovation Institute**, **P.O.Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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 **Mirath**;

☐ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Mirath**, 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:

Title:

Date: 31.01.25

Place: Hattingen, Germany



I, **Gora Adj**, of **Technology Innovation Institute, P.O. Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, am the owner of the **Mirath** 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: Gora Adj

Title: Dr.

Date: 31/01/2025

Place: Abu Dhabi, United Arab Emirates

A handwritten signature in black ink, consisting of a stylized, elongated horizontal stroke with a vertical line extending downwards from the center, and a small loop at the top right.

I, **Aragon Nicolas, from the University of Limoges**, am the owner of the **Mirath** 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: PhD

Date: 15/01/25

Place: Limoges

A handwritten signature in blue ink, appearing to read 'Aragon', followed by a stylized flourish.

I, **Stefano Barbero**, of the **Politecnico di Torino, Corso Duca degli Abruzzi, 24, 10129 Torino TO, Italy**, am the owner of the **Mirath** 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:

A handwritten signature in black ink that reads "Stefano Barbero". The signature is written in a cursive, slightly slanted style.

Title: Ph. D.

Date: January 15, 2025

Place: Torino, Italy

I, **Magali Bardet, LITIS, Université de Rouen Normandie, avenue de l'Université, 76800**

Saint-Étienne-du-Rouvray, am the owner of the **Mirath** 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: Magali BARDET
Title: Maître de conférences
Date: 17/01/2025
Place: Rouen, France

A handwritten signature in black ink, appearing to read 'Magali Bardet', with a horizontal line underneath.

I, **Emanuele Bellini**, Technology Innovation Institute, Abu Dhabi, UAE, am the owner of the **Mirath** 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: Dr. Emanuele Bellini

Date: 15/01/2025

Place: Abu Dhabi

I, **Loïc Bidoux**, **Technology Innovation Institute**, **P.O.Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, am the owner of the **Mirath** 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: Loïc Bidoux

Title: Dr

Date: 15/01/2025

Place: Abu Dhabi

A handwritten signature in black ink, consisting of a stylized capital letter 'B' with a horizontal line extending to the left and another extending to the right, crossing the vertical stem of the 'B'.

I, **Jesús Javier Chi Domínguez, Technology Innovation Institute, P.O. Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, am the owner of the **Mirath** 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: Jesús Javier Chi Domínguez
Title: Dr.
Date: 15/01/2025
Place: Abu Dhabi, UAE



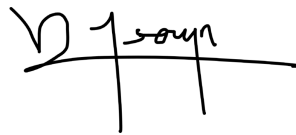
I, **Victor DYSERYN**, of **Télécom Paris, 19, place Marguerite Perey, 91120 Palaiseau, FRANCE**, am the owner of the **Mirath** submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works 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: Victor DYSERYN


Title: Dr.

Date: January 15, 2025

Place: Palaiseau

A handwritten signature in black ink, appearing to read 'V DYSERYN', written over a horizontal line.

I, **Andre Esser, Technology Innovation Institute, P.O.Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, am the owner of the **Mirath** 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: PhD

Date: 15th January 2025

Place: Abu Dhabi

I, **Thibault Feneuil, CryptoExperts, 41 Boulevard des Capucines, 75002 Paris, France**, am the owner of the **Mirath** 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: Thibault Feneuil

Title: Dr.

Date: 15/01/2025

Place: Paris, France

A handwritten signature in black ink. The first part of the signature is 'Thibault' written in a cursive style. Below it, the name 'FENEUIL' is written in all capital letters, underlined with a long horizontal stroke that extends to the right.

I, **Philippe Gaborit**, **University of Limoges**, **123 avenue Albert Thomas**, **87000 Limoges**, **France**, am the owner of the **Mirath** 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: Philippe gaborit

Title: Professor

Date: January 15 2025

Place: Limoge, France

P. Gaborit.

A handwritten signature in blue ink, appearing to be 'P. Gaborit', with a long horizontal stroke extending to the right.

I, **Romaric NEVEU**, **XLIM**, **123 Avenue Albert Thomas**, **87000 Limoges**, **France**, am the owner of the **Mirath** 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: Romaric NEVEU

Title: Mr.

Date: January 15 2025

Place: Limoges

A handwritten signature in black ink, appearing to read 'R Neveu', is positioned to the right of the signature text.

I, **Matthieu Rivain**, of **CryptoExperts, 41 boulevard des Capucines, 75002 Paris**, am the owner of the **Mirath** 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: Matthieu Rivain

Title: Dr.

Date: 20/01/2025

Place: Paris

A handwritten signature in black ink, consisting of a stylized 'M' and 'R' intertwined.

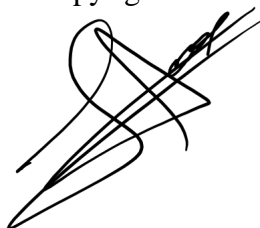
I, **Luis Alberto Rivera Zamarripa, Technology Innovation Institute, P.O. Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates**, am the owner of the **Mirath** submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to 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: Luis Alberto Rivera Zamarripa

Title: Dr.

Date: 24/01/2025

Place: Abu Dhabi, UAE

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.

I, **Carlo Sanna**, of the **Politecnico di Torino, Corso Duca degli Abruzzi, 24, 10129 Torino TO, Italy**, am the owner of the **Mirath** 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:

A handwritten signature in black ink that reads "Carlo Sanna". The signature is written in a cursive, flowing style.

Title: PhD

Date: January 15, 2025

Place: Torino, Italy

I, **Jean-Pierre TILLICH**, from **Inria, 48 rue Barrault Paris 75012, FRANCE** , am the owner of the **Mirath** 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: Jean-Pierre Tillich

Title: Dr.

Date: February 3rd 2025

Place: Paris

A handwritten signature in black ink, appearing to read 'J. Tillich', with a long horizontal stroke extending to the left.

I, **Javier Alfonso Verbel Herrera Technology Innovation Institute, P.O.Box:9639, Yas Island, Abu Dhabi, United Arab Emirates**, am the owner of the **Mirath** 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:

A handwritten signature in black ink that reads "Javier Verbel H.".

Title: Dr

Date: January 15th, 2025

Place: Abu Dhabi, United Arab Emirates

I, **Floyd Zweydinger, Technology Innovation Institute, P.O.Box: 9639, Yas Island Abu Dhabi, United Arab Emirates**, am the owner of the **Mirath** 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:

Date: 31.01.25

Place: Hattingen, Germany

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke extending to the right.