

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 Dyseryn, University of Limoges
Andre Esser, Technology Innovation Institute, UAE
Thibauld 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 Zweydinger, 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, appearing to read "Gora Adj". The signature is fluid and cursive, with a prominent vertical stroke on the right side.

Signed:

Title: PhD

Date: January 15, 2025

Place: Limoges

A handwritten signature in blue ink, appearing to read "Amaury".

Signed:

Stefano Borlenghi

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". The signature is fluid and cursive, with a small flourish at the beginning.

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, appearing to read "Loïc Bidoux". The signature is written over two horizontal lines.

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 Javier Chi Domínguez".

Signed: Victor DYSERYN

Title: Dr.

Date: January 15, 2025

Place: Palaiseau



A handwritten signature in black ink, appearing to read "Victor DYSERYN". The signature is written in a cursive style with a horizontal line through it.

Signed: *A. h*

Title: PhD

Date: 15th January 2025

Place: Abu Dhabi

Signed: Thibauld Feneuil

Title: Dr.

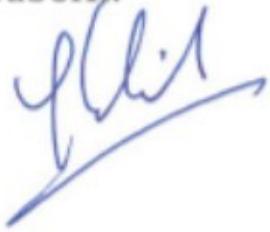
Date: 15/01/2025

Place: Paris, France

Thibaud
FENEUIL

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

P. Gaborit.

A handwritten signature in blue ink, appearing to read "P. Gaborit". The signature is fluid and cursive, with a distinct upward flourish at the end.

Signed: Romaric NEVEU

Title: Mr.

Date: January 15 2025

Place: Limoges

R Neveu

Signed: Matthieu Rivain

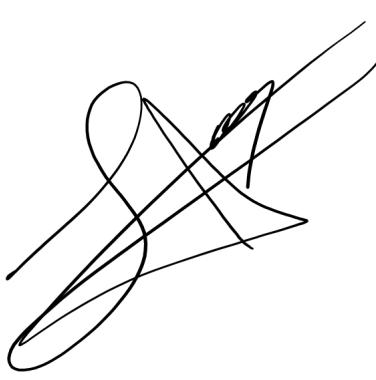
Title: Dr.

Date: 20/01/2025

Place: Paris

A handwritten signature in black ink, appearing to read "Matthieu Rivain".

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



Signed:

A handwritten signature in black ink, appearing to read "Carlo Sanna".

Title: PhD

Date: January 15, 2025

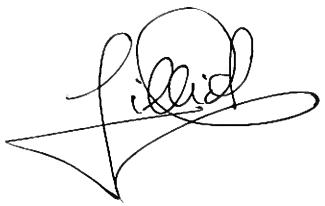
Place: Torino, Italy

Signed: Jean-Pierre Tillich

Title: Dr.

Date: February 3rd 2025

Place: Paris

A handwritten signature in black ink, appearing to read "Tillich". The signature is fluid and cursive, with a large loop at the top and a downward stroke at the bottom.

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 loops and strokes, positioned above the text.A small, faint, roughly circular mark or hole punch on the paper.

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**.

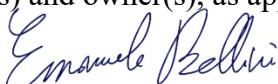
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government 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



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



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, **Thibauld 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: Thibauld Feneuil

Title: Dr.

Date: 15/01/2025

Place: Paris, France



A handwritten signature in black ink, reading "Thibaud FENEUIL". The signature is written in a cursive style with a horizontal line extending from the left and another from the right, enclosing the name.

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.

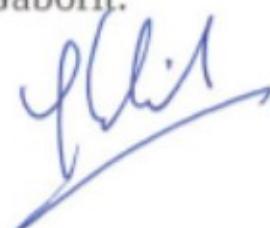
I acknowledge that, during the post-quantum algorithm evaluation process, NIST may remove my cryptosystem from consideration for standardization. If my cryptosystem (or the derived cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and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

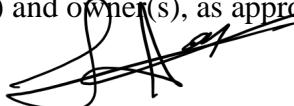
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government 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, appearing to read "Gora Adj".

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 surname.

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, reading "Stefano Barbero". The signature is fluid and cursive, with "Stefano" on the left and "Barbero" on the right, separated by a small gap.

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".

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, appearing to read "L. Bidoux". It consists of a stylized 'L' followed by 'Bidoux' with a small 'B' and 'd'.

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

A handwritten signature in blue ink, appearing to read "Jesús Javier Chi Domínguez".

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 "Victor DYSERYN". The signature is written in a cursive style with a horizontal line through it.

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

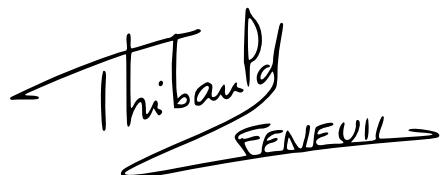
I, Thibauld Feneuil, CryptoExperts, 41 Boulevard des Capucines, 75002 Paris, France, am the owner of the Mirath submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, prepare derivative works based upon, distribute 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: Thibauld Feneuil

Title: Dr.

Date: 15/01/2025

Place: Paris, France

A handwritten signature in black ink. The name "Thibauld" is written in cursive across the top, with a small "D" at the end. Below it, the surname "FENEUIL" is written in capital letters, also in cursive, enclosed within a large, sweeping underline.

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 read "P. Gaborit".

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".

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, appearing to read "Matthieu Rivain".

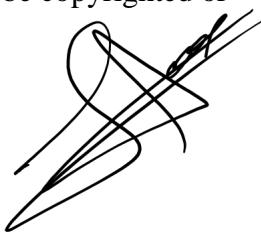
I, Luis Alberto Rivera Zamarripa, Technology Innovation Institute, P.O. Box: 9639, Yas Island, Abu Dhabi, United Arab Emirates, am the owner of the **Mirath** submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to reproduce, 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, appearing to read "Luis Alberto Rivera Zamarripa". The signature is fluid and cursive, with a large, stylized 'L' at the beginning.

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 style with a fluid, continuous flow of lines.

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 "Jean-Pierre Tillich".

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, appearing to read "Javier Verbel H."

Title: Dr

Date: January 15th, 2025

Place: Abu Dhabi, United Arab Emirates

I, Floyd Zweyding, 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

