

I, **Muhammad Reza Z'aba**, of **Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

- 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 **CiliPadi**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi**, 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

A handwritten signature in black ink, appearing to be 'Z. J. ...', written over a horizontal line.

Title: **Dr.**

Date: **26 February 2019**

Place: **University of Malaya, Kuala Lumpur, Malaysia**

I, **Muhammad Reza Z'aba**, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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 be 'MRZ' with a flourish at the end.

Title: **Dr.**

Date: **26 February 2019**

Place: **University of Malaya, Malaysia**

I, **Norziana Jamil**, of **College of Computing and Informatics, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi**, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

- 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 **CiliPadi**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi**, 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

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

Title: **Dr.**

Date: **19 February 2019**

Place: **College of Computing and Informatics, Universiti Tenaga Nasional, Jalan IKRAM-UNITEN, 43000 Kajang, Selangor, Malaysia**

I, Mohd Saufy Rohmad , Faculty of Electrical Engineering, Universiti Teknologi MARA Shah Alam Selangor MALAYSIA , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as CiliPadi , is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):



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 Cilipadi;

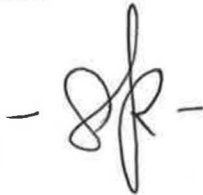
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Cilipadi, may be covered by the following U.S. and/or foreign patents: none;
- I do hereby declare that, to the best of my knowledge, the following pending 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

A handwritten signature in black ink, consisting of a stylized 'S' followed by a vertical line and a horizontal line, with a dash on the left and a dash on the right.

Title: **Mr**

Date: **19 February 2019**

Place: **No 11, Jalan P9A/3 62250 Putrajaya MALAYSIA**

I, Mohd Saufy Rohmad, Faculty of Electrical Engineering, Universiti Teknologi MARA 40450 Shah Alam, Selangor, Malaysia , am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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 be 'Saufy Rohmad', written over a horizontal line. The signature is stylized and cursive.

Title: **Mr**

Date: **19 February 2019**

Place: **No 11, Jalan P9A/3 62550 Putrajaya, MALAYSIA**

I, **Hazlin Abdul Rani**, of **CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi** is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

- 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 **CiliPadi**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi** 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 

Title: -

Date: **26th February 2019**

Place: **CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**

I, **Hazlin Abdul Rani, CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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: **26th February 2019**

Place: **CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**

I, **Solahuddin Shamsuddin**, of **CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi** is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that (check at least one of the following):

- 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 **CiliPadi**;
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **CiliPadi** 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 2.4.2 and 2.4.3, 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 lightweight crypto 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 2.4.1, 2.4.2 and 2.4.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed:

A handwritten signature in black ink, appearing to be 'J. Lee' or similar, written in a cursive style.

Title: **Dr.**

Date: **19th February 2019**

Place: **CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**

I, **Solahuddin Shamsuddin, CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**, am the owner or authorized representative of the owner (print full name, if different than the signer) of the submitted reference implementation, optimized and additional 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 lightweight cryptography 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.**

Date: **19th February 2019**

Place: **CyberSecurity Malaysia, Level 5 Sapura@Mines, No.7 Jalan Tasik, 43300 Seri Kembangan Selangor, Malaysia**