Submitter's statement

I, Christof Beierle, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Christof Beierle Christof
Title: Dr.
Date: 12th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Christof Beierle, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg, am the owner 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: Christof Beierle
Title: Dr.
Date: 12th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Submitter's statement

I, Alex Biryukov, of 6 Avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Alex Biryukov
Title: Prof. Dr.
Date: 15th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Alex Biryukov, of 6 Avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg, am the owner 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: Alex Biryukov
Title: Prof. Dr.
Date: 15th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Submitter's statement

I, Luan Cardoso dos Santos, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Luan Cardoso dos Santos
Title: MSc.
Date: 12th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Luan Cardoso dos Santos, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg, am the owner 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: Luan Cardoso dos Santos
Title: MSc.
Date: 12th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Submitter's statement

I, Johann Großschädl, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Johann Großschädl
Title: M.Sc.
Date: 15th February 2019
Place: Esch-sur-Alzette, Luxembourg

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Johann Großschädl, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, am the owner 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: Johann Großschädl Johann Großschädl
Title: M.Sc.
Date: 15th February 2019
Place: Esch-sur-Alzette, Luxembourg

Submitter's statement

I, Léo Perrin, of 2 rue Simone Iff, 75012 Paris, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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 SPARKLE (along with ESCH and SCHWAEMM);

✓ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with ESCH and SCHWAEMM), 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: Léo Perrin
Title: Dr.
Date: 6th of February 2019
Place: Paris, France

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Léo Perrin, of 2 rue Simone Iff, 75012 Paris, 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: Léo Perrin
Title: Dr.
Date: 6th of February 2019
Place: Paris, France

Submitter's statement

I, Aleksei Udovenko, of 6 Avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Aleksei Udovenko
Title: Mr.
Date: 14th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Aleksei Udovenko, of 6 Avenue de la Fonte, L-4364 Esch-sur-Alzette, Luxembourg, am the owner 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: Aleksei Udovenko
Title: Mr.
Date: 14th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Submitter's statement

I, Qingju Wang, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Qingju Wang
Title: Dr.
Date: 15th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Qingju Wang, of 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, am the owner 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: Qingju Wang 王庆菊
Title: Dr.
Date: 15th of February 2019
Place: Esch-sur-Alzette, Luxembourg

Submitter's statement

I, Vesselin Velichkov, of 10 Crichton St., Edinburgh, EH8 9AB, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Vesselin Velichkov
Title: Dr.
Date: 7th of February 2019
Place: Edinburgh, Scotland

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, Vesselin Velichkov, of 10 Crichton St., Edinburgh, EH8 9AB, am the owner 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: Vesselin Velichkov
Title: Dr.
Date: 7th of February 2019
Place: Edinburgh, Scotland

Submitter's statement

I, *Aein Rezaei Shahmirzadi*, of ID 2-619, *Security Engineering Group, Ruhr-Universitaet Bochum, Universitaetsstr. 150, 44780, Bochum, Germany,* do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Aein Rezaei
Title: —
Date: 12.05.2021
Place: Bochum, Germany

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, *Aein Rezaei Shahmirzadi*, of *ID 2-619, Security Engineering Group, Ruhr-Universitaet Bochum, Universitaetsstr. 150, 44780, Bochum, Germany*, am the owner 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: Aein Rezaei
Title: –
Date: 12.05.2021
Place: Bochum, Germany

Submitter's statement

I, *Amir Moradi*, of ID 2-605, *Security Engineering Group, Ruhr-Universitaet Bochum, Universitaetsstr. 150, 44780, Bochum, Germany,* do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

I further declare that:

- 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 SPARKLE (along with ESCH and SCHWAEMM);
- to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as SPARKLE (along with the hash function ESCH and the authenticated cipher SCHWAEMM), 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: Prof.
Date: 12.05.2021
Place: Bochum, Germany.

Statement by Reference/Optimized/Additional Implementations' Owner(s)

I, *Amir Moradi*, of *ID 2-605, Security Engineering Group, Ruhr-Universitaet Bochum, Universitaetsstr. 150, 44780, Bochum, Germany*, am the owner 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: Prof.
Date: 12.05.2021
Place: Bochum, Germany