Statement by submitter

I, Daniel Penazzi, of Famaf-Universidad Nacional de Córdoba, CIEM, Haya de la Torre s/n, Ciudad Universitaria, Córdoba, Argentina, do hereby declare that the cryptosystem, reference implementation, and optimized implementations that I have submitted, known as Shamash, is the original work of the joint submitters: myself and Miguel Montes.

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 Shamash;

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

DPenazzi

Signed: Daniel Penazzi
Title: Associate Professor, FAMAF, UNC
Date: February 25, 2019
Place: Córdoba, Argentina

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

I, Daniel Penazzi, Famaf-Universidad Nacional de Córdoba, CIEM, Haya de la Torre s/n, Ciudad Universitaria, Córdoba, Argentina, 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: Daniel Penazzi
Title: Associate Professor, FAMAF, UNC
Date: February 25, 2019
Place: Córdoba, Argentina

Statement by submitter

I, Daniel Penazzi, of Famaf-Universidad Nacional de Córdoba, CIEM, Haya de la Torre s/n, Ciudad Universitaria, Córdoba, Argentina, do hereby declare that the cryptosystem, reference implementation, and optimized implementations that I have submitted, known as Shamashash, is the original work of the joint submitters: myself and Miguel Montes.

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 Shamashash;

✓ to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Shamash, 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: Daniel Penazzi
Title: Associate Professor, FAMAF, UNC
Date: February 25, 2019
Place: Córdoba, Argentina

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

I, Daniel Penazzi, Famaf-Universidad Nacional de Córdoba, CIEM, Haya de la Torre s/n, Ciudad Universitaria, Córdoba, Argentina, 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.

DPenazzi

Signed: Daniel Penazzi
Title: Associate Professor, FAMAF, UNC
Date: February 25, 2019
Place: Córdoba, Argentina

Statement by submitter

I, Miguel Montes, of Blamey Lafore 1276, Córdoba, Argentina, do hereby declare that the cryptosystem, reference implementation, and optimized implementations that I have submitted, known as Shamash, is the original work of the joint submitters: Daniel Penazzi and myself.

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 Shamash.

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Shamash, 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: Miguel Montes
Title: Professor, UNDEF - CRUC IUA
Date: February 25, 2019
Place: Córdoba, Argentina

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

I, Miguel Montes, Blamey Lafore 1276, Córdoba, Argentina, 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: Miguel Montes
Title: Professor, UNDEF, CRUC IUA
Date: February 25, 2019
Place: Córdoba, Argentina

Statement by submitter

I, Miguel Montes, of Blamey Lafore 1276, Córdoba, Argentina, do hereby declare that the cryptosystem, reference implementation, and optimized implementations that I have submitted, known as Shamashash, is the original work of the joint submitters: Daniel Penazzi and myself.

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 Shamashash.

to the best of my knowledge, the practice of the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Shamashash, 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: Miguel Montes
Title: Professor, UNDEF - CRUC IUA
Date: February 25, 2019
Place: Córdoba, Argentina

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

I, Miguel Montes, Blamey Lafore 1276, Córdoba, Argentina, 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: Miguel Montes
Title: Professor, UNDEF, CRUC IUA
Date: February 25, 2019
Place: Córdoba, Argentina