COVER SHEET

Name of the proposed cryptosystem: Mersenne-756839

Principal submitter's name: Divesh Aggarwal

e-mail address: divesh.aggarwal@gmail.com

Telephone: +65-92729378

Postal address: Centre for Quantum Technologies, S15, 3 Science Drive 2, 117543 Singapore

Names of auxiliary submitters: Antoine Joux, Anupam Prakash, Miklos Santha

Names of the inventors/developers of the cryptosystem: Divesh Aggarwal, Antoine Joux, Anupam Prakash, Miklos Santha

Names of the owners of the cryptosystem: Divesh Aggarwal, Antoine Joux, Anupam Prakash, Miklos Santha

Signature of the submitter: 

Backup point of contact: Antoine Joux, of Fondation Partenariale UPMC, 4 Place Jussieu, 75005 Paris, France, phone: +33-667358228, e-mail: Antoine.Joux@m4x.org

I, Antoine Joux, of Fondation Partenariale UPMC, 4 Place Jussieu, 75005 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Mersenne-756839, is my own original work, or if submitted jointly with others, is the original work of the joint submitters.

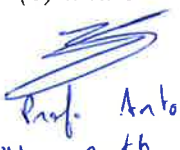
I further declare that I do not hold and do not intend to hold any patent or patent application with a claim which may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Mersenne-756839;

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: Prof. Antoine Joux

Date: Nov. 20th, 2017

Place: Paris

I, Anupam Prakash, of School of Mathematical and Physical Sciences, 21 Nanyang Link, Nanyang Technological University, Singapore- 637371 and Centre for Quantum Technologies, Block S15, 3 Science Drive 2, National University of Singapore, Singapore - 117543, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Mersenne-756839, 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 Mersenne-756839;

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: Prakash

Title: Dr.

Date: 17 November 2017

Place: Singapore

I, Miklos Santha, of CNRS, IRIF, Université Paris Diderot, Case 7014, 75205 Paris, France and Centre for Quantum Technologies, National University of Singapore, S15, 3 Science Drive 2, 117543 Singapore, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Mersenne-756839, 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 Mersenne-756839;

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: Miklos Santha

Title: Dr.

Date: November 17, 2017

Place: Singapore

I, Divesh Aggarwal, of School of Computing and Centre for Quantum Technologies, S15, 3 Science Drive 2, 117543 Singapore, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Mersenne-756839, 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 Mersenne-756839;

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: Divesh

Title: Dr.

Date: NOVEMBER 17, 2017

Place: SINGAPORE

I, Antoine Joux, of Foundation Partenariale UPMC, 4 Place Jussieu, 75005 Paris, France, am the owner or authorized representative of the owner (print full name, if different than the signer) of the 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: Prof. Antoine JOUX

Date: Nov. 20th, 2017

Place: Paris.