Lepton [1]: Key Encapsulation Mechanisms from a variant of Learning Parity with Noise

Name: Lepton

Principal submitters: Yu Yu, Shanghai Jiao Tong University, China
Jiang Zhang, State Key Laboratory of Cryptology, China

Inventors: Yu Yu, Shanghai Jiao Tong University, China
Jiang Zhang, State Key Laboratory of Cryptology, China

Owners: Yu Yu, Shanghai Jiao Tong University, China
Jiang Zhang, State Key Laboratory of Cryptology, China

Contact information: Yu Yu & Jiang Zhang
Postal addresses: #4-2803, 688 South Xizang Rd, Shanghai, China 200011
P.O. Box 5159, Beijing, China 100878
E-mail addresses: yyuu@sjtu.edu.cn jiangzhang09@gmail.com
Contact numbers: +86-15000088966 +86-15110204521

Date: November 28, 2017

Signature:

[1] The design and analysis of the Lepton crypto-system [51] are based on preliminary results obtained in [52], which is currently in submission and will appear in IACR ePrint at an appropriate time.

2.D.1 Statement by Each Submitter

I, _____Yu Yu_____, of _#4-2803, 688 South Xizang Rd, Shanghai, China 200011 ____ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____Lepton____, 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 ____ Lepton___; **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 _Lepton____, 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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 郁昱
Title: Dr.
Date: November 20, 2017
Place: Shanghai, China

2.D.1 Statement by Each Submitter

I, _____Jiang Zhang_____, of _ P.O. Box 5159, Beijing, China 100878 ____ , do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as ____Lepton____, 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 ____ Lepton___; **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 _Lepton____, 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 in the Call For Proposals 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 of the Call For Proposals, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: 张江
Title: Dr.
Date: November 20, 2017
Place: Beijing, China

2.D.3 Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, _____Jiang Zhang_____ , P.O. Box 5159, Beijing, China 100878_____ , am the owner 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: 张江
Title: Dr.
Date: November 20, 2017
Place:Beijing, China