Statement by Each Submitter

I, Thomas Prest, of PQShield SAS, 259 rue Saint Honoré, 75001 Paris, France, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon, 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 or that could be amended to include a claim that may cover the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as Raccoon;

☑ to the best of my knowledge, the following pending U.S. and/or foreign patent applications may cover the practice of Raccoon, reference implementation or optimized implementations: _____ (describe and enumerate or state "none" if applicable) _____.

- **Title:** Lattice-based cryptographic digital signature scheme utilising masking

  Abstract: The present invention relates to a cryptographic digital signature scheme to verify the integrity and origin of an electronic message. The invention has relevance to a post-quantum lattice-based cryptographic digital signature scheme utilising masking as a countermeasure to side channel attacks.

  Application number: PCT/EP2023/052730

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: Thomas Prest

Title: Lead cryptography researcher

Date: 31 May 2023

Place: Paris, France