2.D.1 Statement by Each Submitter

*I, **Anubhab Baksi**, of **Temasek Laboratories, Nanyang Technological University, 50 Nanyang Drive, Research Techno Plaza, Border X Block, Level 8, Singapore 637553**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Ascon-Sign**, 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 **Ascon-Sign**; **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 _____ **(print name of cryptosystem)**_____, may be covered by the following U.S. and/or foreign patents: _____ **(describe and enumerate or state "none" if applicable)**_____ ;*

- *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: _____ **(describe and enumerate or state "none" if applicable)** _____ .*

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: Anubhab Baksi
Title: Dr.
Date: 1 June 2023
Place: Singapore

2.D.1 Statement by Each Submitter

I, **Arpan Jati**, of **Nanyang Technological University, Singapore**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Ascon-Sign**, 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 **Ascon-Sign**; **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 ____ **(print name of cryptosystem)**____, may be covered by the following U.S. and/or foreign patents: _____ **(describe and enumerate or state "none" if applicable)**_____ ;

- 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: _____ **(describe and enumerate or state "none" if applicable)** _____.

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: Arpan Jati
Title: Research Associate
Date: 1 June 2023
Place: Singapore

2.D.1 Statement by Each Submitter

I, ***Naina Gupta***, *of* ***Temasek Labs, NTU, Singapore***, *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* ***Ascon-Sign***, *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* ***Ascon-Sign***; ***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 ____* ***(print name of cryptosystem)***____*, may be covered by the following U.S. and/or foreign patents:* _____ ***(describe and enumerate or state "none" if applicable)***_____ *;*

- *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:* _____ ***(describe and enumerate or state "none" if applicable)*** _____ *.*

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: Naina Gupta
Title: Research Associate
Date: 1 June 2023
Place: Singapore

2.D.1 Statement by Each Submitter

*I, **Vikas Srivastava**, of **Department of Mathematics**, **National Institute of Technology Jamshedpur, Adityapur-2, 831014, India**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Ascon-Sign** , 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 **Ascon-Sign**; **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 ____ **(print name of cryptosystem)**____ , may be covered by the following U.S. and/or foreign patents: _____ **(describe and enumerate or state "none" if applicable)**____ ;*

- *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: _____ **(describe and enumerate or state "none" if applicable)** _____ .*
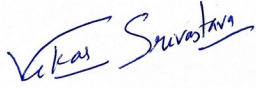
I do hereby acknowledge and agree that my submitted cryptosystem will be provided to the public for review and will be evaluated by NIST, and that it might not be selected for standardization by NIST. I further acknowledge that I will not receive financial or other compensation from the U.S. Government 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: Vikas Srivastava
Title: Ph.D. Student
Date: 1 June 2023
Place: Le Bourget, Paris, France

2.D.1 Statement by Each Submitter

I, **Anupam Chattopadhyay**, *of* **School of Computer Science and Engineering, Block N4, Nanyang Technological University, Singapore 639798**, *do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as* **Ascon-Sign**, *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* **Ascon-Sign**; **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 ____* **(print name of cryptosystem)____**, *may be covered by the following U.S. and/or foreign patents: ____* **(describe and enumerate or state "none" if applicable)____** ;

- *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: ____* **(describe and enumerate or state "none" if applicable)____** .

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
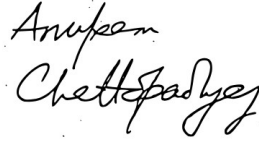
cryptosystem) is removed from consideration for standardization or withdrawn from consideration by all submitter(s) and owner(s), I understand that rights granted and assurances made under Sections 2.D.1, 2.D.2 and 2.D.3, including use rights of the reference and optimized implementations, may be withdrawn by the submitter(s) and owner(s), as appropriate.

Signed: Anupam Chattopadhyay
Title: Associate Professor
Date: 1 June 2023
Place: Singapore

2.D.1 Statement by Each Submitter

*I, **Xiaolu Hou**, of **04-03, Faculty of Informatics and Information Technologies, Slovak University of Technology, Bratislava**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Ascon-Sign**, 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 **Ascon-Sign**; **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 ____ **(print name of cryptosystem)**____, may be covered by the following U.S. and/or foreign patents: _____ **(describe and enumerate or state "none" if applicable)**_____ ;*

- *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: _____ **(describe and enumerate or state "none" if applicable)** _____ .*

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: Xiaolu Hou
Title: Dr.
Date: 1 June 2023
Place: Bratislava

2.D.1 Statement by Each Submitter

*I, **Jakub Breier**, of **Silicon Austria Labs, Graz, Austria**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Ascon-Sign**, 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 **Ascon-Sign**; **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 ____ **(print name of cryptosystem)**____, may be covered by the following U.S. and/or foreign patents: _____ **(describe and enumerate or state "none" if applicable)**_____ ;*

- *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: _____ **(describe and enumerate or state "none" if applicable)** _____ .*

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: Jakub Breier
Title: Dr.
Date: 1 June 2023
Place: Graz, Austria

2.D.1 Statement by Each Submitter

*I, **Sumit Kumar Debnath**, of **Department of Mathematics**, **National Institute of Technology Jamshedpur, Adityapur-2, 831014, India**, do hereby declare that the cryptosystem, reference implementation, or optimized implementations that I have submitted, known as **Ascon-Sign**, 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 **Ascon-Sign**;* **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 _____ (**print name of cryptosystem**)_____, may be covered by the following U.S. and/or foreign patents: _____ (**describe and enumerate or state "none" if applicable**)_____ ;*

- *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: _____ (**describe and enumerate or state "none" if applicable**) _____ .*

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: Sumit Kumar Debnath
Title: Dr.
Date: 1 June 2023
Place: Jamshedpur, India

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

The following must also be included:

*I, **Naina Gupta**, **Nanyang Technological University, Singapore** 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: Naina Gupta
Title: Research Associate
Date: 1 June 2023
Place: Singapore

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

The following must also be included:

*I, **Arpan Jati**, **Nanyang Technological University, Singapore** 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: Arpan Jati
Title: Research Associate
Date: 1 June 2023
Place: Singapore

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

The following must also be included:

*I, **Vikas Srivastava**, **Department of Mathematics, National Institute of Technology Jamshedpur, Adityapur-2, 831014, India** 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: Vikas Srivastava
Title: Ph.D. Student
Date: 1 June 2023
Place: Le Bourget, Paris,
France