

**Statement by Patent (and Patent Application) Owner(s)**

*I, Guido Bertoni, of STMicroelectronics Via Olivetti 2 20041 Agrate - Italy , am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and or patent application(s): NONE, and do hereby agree to grant to any interested party if the algorithm known as KECCAK is selected for SHA-3, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the optimized implementations. Furthermore, I agree to grant the same rights in any other patent application or patent granted to me or my company that may be necessary for the practice of the referenced algorithm, reference implementation, or the optimized implementations.*

Signed: *Guido Bertoni*

Title: Dr

Dated: August 6, 2008

Place: Agrate B.za, Italy

**Statement by Reference/Optimized Implementations' Owner(s)**

*I, Guido Bertoni, 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 use such implementations for the purposes of the SHA-3 evaluation process, notwithstanding that the implementations may be copyrighted.*

Signed: *Guido Bertoni*

Title: Dr

Dated: August 6, 2008

Place: Agrate B.za, Italy

## Statement by the Submitter

*I, Guido Bertoni do hereby declare that, to the best of my knowledge, the practice of the algorithm, reference implementation, and optimized implementations that I have submitted, known as Keccak, may be covered by the following U.S. and/or foreign patents: NONE .*

*I do hereby declare that I am aware of no patent applications that may cover the practice of my submitted algorithm, reference implementation or optimized implementations.*

*I do hereby understand that my submitted algorithm may not be selected for inclusion in the Secure Hash Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for SHA-3. I further understand that I will not receive financial 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 relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the SHS or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for SHA-3, I hereby agree not to place any restrictions on the use of the algorithm, intending it to be available on a worldwide, non-exclusive, royalty-free basis.*

*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 algorithm, reference implementation or optimized implementations and the right to use such implementations for the purposes of the SHA-3 evaluation process.*

*I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for SHA-3 (including those that are not selected for the second round of public evaluation), I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner[s], as appropriate). Additionally, should the U.S. Government not select my algorithm for SHA-3 at the time NIST ends the competition, all rights revert to the submitter (and other owner[s] as appropriate).*

Signed:

*Guido Bertoni*

Title: Dr

Dated: August 6, 2008

Place: Agrate B.za, Italy

## Statement by the Submitter

*I, Joan Daemen do hereby declare that, to the best of my knowledge, the practice of the algorithm, reference implementation, and optimized implementations that I have submitted, known as Keccak, may be covered by the following U.S. and/or foreign patents: NONE .*

*I do hereby declare that I am aware of no patent applications that may cover the practice of my submitted algorithm, reference implementation or optimized implementations.*

*I do hereby understand that my submitted algorithm may not be selected for inclusion in the Secure Hash Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for SHA-3. I further understand that I will not receive financial 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 relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the SHS or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for SHA-3, I hereby agree not to place any restrictions on the use of the algorithm, intending it to be available on a worldwide, non-exclusive, royalty-free basis.*

*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 algorithm, reference implementation or optimized implementations and the right to use such implementations for the purposes of the SHA-3 evaluation process.*

*I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for SHA-3 (including those that are not selected for the second round of public evaluation), I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner[s], as appropriate). Additionally, should the U.S. Government not select my algorithm for SHA-3 at the time NIST ends the competition, all rights revert to the submitter (and other owner[s] as appropriate).*

Signed:

Title: Dr



Dated: August 6, 2008

Place: Zaventem, Belgium

**Statement by Reference/Optimized Implementations' Owner(s)**

*I, Joan Daemen, 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 use such implementations for the purposes of the SHA-3 evaluation process, notwithstanding that the implementations may be copyrighted.*

Signed: 

Title: Dr

Dated: August 6, 2008

Place: Zaventem, Belgium

**Statement by Patent (and Patent Application) Owner(s)**

*I, Joan Daemen, of STMicroelectronics Excelsiorlaan 44-46, 1930 Zaventem, Belgium, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and or patent application(s): NONE, and do hereby agree to grant to any interested party if the algorithm known as KECCAK is selected for SHA-3, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the optimized implementations. Furthermore, I agree to grant the same rights in any other patent application or patent granted to me or my company that may be necessary for the practice of the referenced algorithm, reference implementation, or the optimized implementations.*

Signed:

Title: Dr

Dated: August 6, 2008

Place: Zaventem, Belgium

*Joan Daemen*

**Statement by Patent (and Patent Application) Owner(s)**

I, Michael Peeters, of NXP Semiconductors,  
am the owner or authorized representative of the owner (print full name, if different than  
the signer) of the following patent(s) and or patent application(s): none, and do hereby  
agree to grant to any interested party if the algorithm known as Keccak is selected for  
SHA-3, an irrevocable nonexclusive royalty-free license to practice the referenced  
algorithm, reference implementation or the optimized implementations. Furthermore, I  
agree to grant the same rights in any other patent application or patent granted to me or  
my company that may be necessary for the practice of the referenced algorithm,  
reference implementation, or the optimized implementations.

Signed: Michael Peeters  
Title: Mr  
Dated: August 20th, 2008  
Place: Leuven, Belgium

**Statement by the Submitter**

I, Michaël Peeters do hereby declare that, to the best of my knowledge, the practice of the algorithm, reference implementation, and optimized implementations that I have submitted, known as Keccak, may be covered by the following U.S. and/or foreign patents: none.

I do hereby declare that I am aware of no patent applications that may cover the practice of my submitted algorithm, reference implementation or optimized implementations. –  
**OR** – I do hereby declare that the following pending patent applications may cover the practice of my submitted algorithm, reference implementation or optimized implementations: \_\_\_\_\_ (describe and enumerate) \_\_\_\_\_.

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Secure Hash Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for SHA-3. I further understand that I will not receive financial 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 relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the SHS or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for SHA-3, I hereby agree not to place any restrictions on the use of the algorithm, intending it to be available on a worldwide, non-exclusive, royalty-free basis.

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 algorithm, reference implementation or optimized implementations and the right to use such implementations for the purposes of the SHA-3 evaluation process.

I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for SHA-3 (including those that are not selected for the second round of public evaluation), I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner[s], as appropriate). Additionally, should the U.S. Government not select my algorithm for SHA-3 at the time NIST ends the competition, all rights revert to the submitter (and other owner[s] as appropriate).

Signed: Michaël Peeters  
Title: Mr  
Dated: August 20<sup>th</sup>, 2008  
Place: Leuven, Belgium

**Statement by Reference/Optimized Implementations' Owner(s)**

*I, Michaël Peeters, 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 use such implementations for the purposes of the SHA-3 evaluation process, notwithstanding that the implementations may be copyrighted.*

Signed: *Michaël Peeters*  
Title: *Mr*  
Dated: *20th August, 2008*  
Place: *Leuven, Belgium*

## Statement by the Submitter

I, Gilles Van Assche do hereby declare that, to the best of my knowledge, the practice of the algorithm, reference implementation, and optimized implementations that I have submitted, known as Keccak, may be covered by the following U.S. and/or foreign patents: none.

I do hereby declare that I am aware of no patent applications that may cover the practice of my submitted algorithm, reference implementation or optimized implementations. –  
**OR** – I do hereby declare that the following pending patent applications may cover the practice of my submitted algorithm, reference implementation or optimized implementations: \_\_\_\_\_ (describe and enumerate) \_\_\_\_\_.

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Secure Hash Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for SHA-3. I further understand that I will not receive financial 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 relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the SHS or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for SHA-3, I hereby agree not to place any restrictions on the use of the algorithm, intending it to be available on a worldwide, non-exclusive, royalty-free basis.

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 algorithm, reference implementation or optimized implementations and the right to use such implementations for the purposes of the SHA-3 evaluation process.

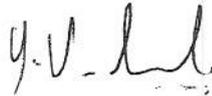
I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for SHA-3 (including those that are not selected for the second round of public evaluation), I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner[s], as appropriate). Additionally, should the U.S. Government not select my algorithm for SHA-3 at the time NIST ends the competition, all rights revert to the submitter (and other owner[s] as appropriate).

Signed: Gilles Van Assche

Title: Dr.

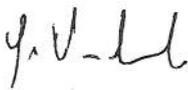
Dated: August 22nd, 2008

Place: Zaventem, Belgium



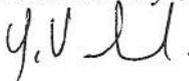
**Statement by Patent (and Patent Application) Owner(s)**

I, Gilles Van Assche, of STMicroelectronics, Excelsiorlaan 44-46, 1930 Zaventem, Belgium, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and or patent application(s): none, and do hereby agree to grant to any interested party if the algorithm known as Keccak is selected for SHA-3, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the optimized implementations. Furthermore, I agree to grant the same rights in any other patent application or patent granted to me or my company that may be necessary for the practice of the referenced algorithm, reference implementation, or the optimized implementations.

Signed: Gilles Van Assche   
Title: Dr.  
Dated: August 22nd, 2008  
Place: Zaventem, Belgium

**Statement by Reference/Optimized Implementations' Owner(s)**

*I, Gilles Van Assche, 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 use such implementations for the purposes of the SHA-3 evaluation process, notwithstanding that the implementations may be copyrighted.*

Signed: Gilles Van Assche 

Title: Dr.

Dated: August 22nd, 2008

Place: Zaventem, Belgium