

Appendix B: Intellectual Property Statements

B.1 Statement by Each Algorithm Submitter

I, Xianhui Lu (full name), No. 19 Shucun Road, Haidian District, Beijing, China (full postal address), to the best of my knowledge of my submitted algorithm CreTAKE (name of algorithm) and its implementations (reference and optimized implementations included), do hereby declare:

1. I commit that my submitted algorithm and its implementations are in compliance with the security requirements, including but not limited to the requirements that the algorithm does not contain any backdoor or defect artificially designed and its implementations do not contain any malicious code. I do hereby commit that to the best of my knowledge, my submitted algorithm and its implementations do not contain any data, information or technology that may infringe upon trade secrets, or may involve confidentiality required by the laws and regulations of China and other countries.
2. I acknowledge and agree that my submitted algorithm and its implementations will be provided to the public for evaluation, analysis and review. I agree that any interested party, including the program organizer, public reviewers, etc., can freely use the algorithm and its implementations for evaluation purpose. I acknowledge that the program organizer will select several algorithms as candidates for the next-round evaluation or the finalists after evaluation and analysis; my submitted algorithm might not be selected as a candidate for the next-round evaluation or the finalist. I acknowledge that I will not receive financial or other compensation from the program organizer for my submitted algorithm.
3. To facilitate the next-generation commercial cryptographic algorithm standardization, I acknowledge and agree that if my submitted algorithm is selected for the finalists, the program organizer may modify the algorithm and its implementations out of security, availability or other considerations. If my submitted algorithm is selected for the finalists and to be standardized, I commit to place no restriction on the worldwide disclosure and free adoption of algorithm and its implementations.
4. I commit that the algorithm and its implementations are my (or my team's) own original work. The implementations of my submitted algorithm ☐ do / ☒ do not adopt code or code libraries requiring authorization by third parties. Except those clearly identified, citations and acknowledgment, all the opinions, words, diagrams and data in the submission are my own (or my team's) original research results, and the submission does not contain any published work from other individual or team.
5. (Please check one of the following two options.)
 - ☐ I do not hold and do not intend to hold any patent or patent application which may cover my submitted algorithm and its implementations, and

to the best of my knowledge, no patent or patent application may cover my submitted algorithm and its implementations.

- ☒ The following patent(s) and patent application(s) may cover my submitted algorithm and its implementations. As for patent(s) and patent application(s) held by myself, I ☒ have submitted / ☐ have not submitted all statements; as for patent(s) and patent application(s) held by others, I ☐ have submitted / ☐ have not submitted all statements signed by patent and patent application owner(s).

Table The List of Patent(s) and Patent Application(s)

No.	Patent/Patent Application No.	Title of Patent/Patent Application	Patent/Patent Application Owner(s)	Whether submit statements signed by each owner
1	202510447608.7	A Heterogeneous Authenticated Key Exchange Method Based on Key Encapsulation Mechanisms and Digital Signatures	Institute of Information Engineering, CAS	☒ Yes ☐ No
2				☐ Yes ☐ No

Note: The algorithm submitter(s) shall fill in the table according to his/her/their situation.

I do hereby declare that to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my submitted algorithm and its implementations. I commit that to the best of my knowledge, my submitted algorithm and its implementations are in compliance with the laws and regulations of China and other countries, and do not infringe upon legitimate rights and interests of any third party. Where there is a dispute concerning patent infringement or violation of laws and regulations, I commit that the algorithm submitter(s) shall take the responsibility of dealing with it and eliminating negative effects as well as bearing corresponding legal liabilities.

I am fully aware that I bear the legal consequences of this statement.

Signed: Xiaohui Lu 徐晓辉

Date: 2026.6.29

(Note: If there are multiple algorithm submitters, the statements shall be signed by each and every one of them.)

B.1 Statement by Each Algorithm Submitter

I, Jingnan He (full name), No. 19 Shucun Road, Haidian District, Beijing, China (full postal address), to the best of my knowledge of my submitted algorithm CreTAKE (name of algorithm) and its implementations (reference and optimized implementations included), do hereby declare:

1. I commit that my submitted algorithm and its implementations are in compliance with the security requirements, including but not limited to the requirements that the algorithm does not contain any backdoor or defect artificially designed and its implementations do not contain any malicious code. I do hereby commit that to the best of my knowledge, my submitted algorithm and its implementations do not contain any data, information or technology that may infringe upon trade secrets, or may involve confidentiality required by the laws and regulations of China and other countries.
2. I acknowledge and agree that my submitted algorithm and its implementations will be provided to the public for evaluation, analysis and review. I agree that any interested party, including the program organizer, public reviewers, etc., can freely use the algorithm and its implementations for evaluation purpose. I acknowledge that the program organizer will select several algorithms as candidates for the next-round evaluation or the finalists after evaluation and analysis; my submitted algorithm might not be selected as a candidate for the next-round evaluation or the finalist. I acknowledge that I will not receive financial or other compensation from the program organizer for my submitted algorithm.
3. To facilitate the next-generation commercial cryptographic algorithm standardization, I acknowledge and agree that if my submitted algorithm is selected for the finalists, the program organizer may modify the algorithm and its implementations out of security, availability or other considerations. If my submitted algorithm is selected for the finalists and to be standardized, I commit to place no restriction on the worldwide disclosure and free adoption of algorithm and its implementations.
4. I commit that the algorithm and its implementations are my (or my team's) own original work. The implementations of my submitted algorithm ☐ do / ☒ do not adopt code or code libraries requiring authorization by third parties. Except those clearly identified, citations and acknowledgment, all the opinions, words, diagrams and data in the submission are my own (or my team's) original research results, and the submission does not contain any published work from other individual or team.
5. (Please check one of the following two options.)
 - ☐ I do not hold and do not intend to hold any patent or patent application which may cover my submitted algorithm and its implementations, and to the best of my knowledge, no patent or patent application may cover my submitted algorithm and its implementations.

- ☒ The following patent(s) and patent application(s) may cover my submitted algorithm and its implementations. As for patent(s) and patent application(s) held by myself, I ☒ have submitted / ☐ have not submitted all statements; as for patent(s) and patent application(s) held by others, I ☐ have submitted / ☐ have not submitted all statements signed by patent and patent application owner(s).

Table The List of Patent(s) and Patent Application(s)

No.	Patent/Patent Application No.	Title of Patent/Patent Application	Patent/Patent Application Owner(s)	Whether submit statements signed by each owner
1	202510447608.7	A Heterogeneous Authenticated Key Exchange Method Based on Key Encapsulation Mechanisms and Digital Signatures	Institute of Information Engineering, CAS	☒ Yes ☐ No
2				☐ Yes ☐ No

Note: The algorithm submitter(s) shall fill in the table according to his/her/their situation.

I do hereby declare that to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my submitted algorithm and its implementations. I commit that to the best of my knowledge, my submitted algorithm and its implementations are in compliance with the laws and regulations of China and other countries, and do not infringe upon legitimate rights and interests of any third party. Where there is a dispute concerning patent infringement or violation of laws and regulations, I commit that the algorithm submitter(s) shall take the responsibility of dealing with it and eliminating negative effects as well as bearing corresponding legal liabilities.

I am fully aware that I bear the legal consequences of this statement.

Signed: Jingnan He 贺婧楠

Date: 2026.6.29

(Note: If there are multiple algorithm submitters, the statements shall be signed by each and every one of them.)

B.1 Statement by Each Algorithm Submitter

I, Yao Cheng (full name), No. 19 Shucun Road, Haidian District, Beijing, China (full postal address), to the best of my knowledge of my submitted algorithm CreTAKE (name of algorithm) and its implementations (reference and optimized implementations included), do hereby declare:

1. I commit that my submitted algorithm and its implementations are in compliance with the security requirements, including but not limited to the requirements that the algorithm does not contain any backdoor or defect artificially designed and its implementations do not contain any malicious code. I do hereby commit that to the best of my knowledge, my submitted algorithm and its implementations do not contain any data, information or technology that may infringe upon trade secrets, or may involve confidentiality required by the laws and regulations of China and other countries.
2. I acknowledge and agree that my submitted algorithm and its implementations will be provided to the public for evaluation, analysis and review. I agree that any interested party, including the program organizer, public reviewers, etc., can freely use the algorithm and its implementations for evaluation purpose. I acknowledge that the program organizer will select several algorithms as candidates for the next-round evaluation or the finalists after evaluation and analysis; my submitted algorithm might not be selected as a candidate for the next-round evaluation or the finalist. I acknowledge that I will not receive financial or other compensation from the program organizer for my submitted algorithm.
3. To facilitate the next-generation commercial cryptographic algorithm standardization, I acknowledge and agree that if my submitted algorithm is selected for the finalists, the program organizer may modify the algorithm and its implementations out of security, availability or other considerations. If my submitted algorithm is selected for the finalists and to be standardized, I commit to place no restriction on the worldwide disclosure and free adoption of algorithm and its implementations.
4. I commit that the algorithm and its implementations are my (or my team's) own original work. The implementations of my submitted algorithm ☐ do / ☒ do not adopt code or code libraries requiring authorization by third parties. Except those clearly identified, citations and acknowledgment, all the opinions, words, diagrams and data in the submission are my own (or my team's) original research results, and the submission does not contain any published work from other individual or team.
5. (Please check one of the following two options.)
 - ☐ I do not hold and do not intend to hold any patent or patent application which may cover my submitted algorithm and its implementations, and to the best of my knowledge, no patent or patent application may cover my submitted algorithm and its implementations.

- ☒ The following patent(s) and patent application(s) may cover my submitted algorithm and its implementations. As for patent(s) and patent application(s) held by myself, I ☒ have submitted / ☐ have not submitted all statements; as for patent(s) and patent application(s) held by others, I ☐ have submitted / ☐ have not submitted all statements signed by patent and patent application owner(s).

Table The List of Patent(s) and Patent Application(s)

No.	Patent/Patent Application No.	Title of Patent/Patent Application	Patent/Patent Application Owner(s)	Whether submit statements signed by each owner
1	202510447608.7	A Heterogeneous Authenticated Key Exchange Method Based on Key Encapsulation Mechanisms and Digital Signatures	Institute of Information Engineering, CAS	☒ Yes ☐ No
2				☐ Yes ☐ No

Note: The algorithm submitter(s) shall fill in the table according to his/her/their situation.

I do hereby declare that to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my submitted algorithm and its implementations. I commit that to the best of my knowledge, my submitted algorithm and its implementations are in compliance with the laws and regulations of China and other countries, and do not infringe upon legitimate rights and interests of any third party. Where there is a dispute concerning patent infringement or violation of laws and regulations, I commit that the algorithm submitter(s) shall take the responsibility of dealing with it and eliminating negative effects as well as bearing corresponding legal liabilities.

I am fully aware that I bear the legal consequences of this statement.

Signed: Yao Cheng 程瑶

Date: 2026.06.29

(Note: If there are multiple algorithm submitters, the statements shall be signed by each and every one of them.)

B.1 Statement by Each Algorithm Submitter

I, Haiyang Xue (full name), 90 Stamford Road, Singapore (full postal address), to the best of my knowledge of my submitted algorithm CreTAKE (name of algorithm) and its implementations (reference and optimized implementations included), do hereby declare:

1. I commit that my submitted algorithm and its implementations are in compliance with the security requirements, including but not limited to the requirements that the algorithm does not contain any backdoor or defect artificially designed and its implementations do not contain any malicious code. I do hereby commit that to the best of my knowledge, my submitted algorithm and its implementations do not contain any data, information or technology that may infringe upon trade secrets, or may involve confidentiality required by the laws and regulations of China and other countries.
2. I acknowledge and agree that my submitted algorithm and its implementations will be provided to the public for evaluation, analysis and review. I agree that any interested party, including the program organizer, public reviewers, etc., can freely use the algorithm and its implementations for evaluation purpose. I acknowledge that the program organizer will select several algorithms as candidates for the next-round evaluation or the finalists after evaluation and analysis; my submitted algorithm might not be selected as a candidate for the next-round evaluation or the finalist. I acknowledge that I will not receive financial or other compensation from the program organizer for my submitted algorithm.
3. To facilitate the next-generation commercial cryptographic algorithm standardization, I acknowledge and agree that if my submitted algorithm is selected for the finalists, the program organizer may modify the algorithm and its implementations out of security, availability or other considerations. If my submitted algorithm is selected for the finalists and to be standardized, I commit to place no restriction on the worldwide disclosure and free adoption of algorithm and its implementations.
4. I commit that the algorithm and its implementations are my (or my team's) own original work. The implementations of my submitted algorithm ☐ do / ☒ do not adopt code or code libraries requiring authorization by third parties. Except those clearly identified, citations and acknowledgment, all the opinions, words, diagrams and data in the submission are my own (or my team's) original research results, and the submission does not contain any published work from other individual or team.
5. (Please check one of the following two options.)
 - ☒ I do not hold and do not intend to hold any patent or patent application which may cover my submitted algorithm and its implementations, and to the best of my knowledge, no patent or patent application may cover my submitted algorithm and its implementations.

- ☐ The following patent(s) and patent application(s) may cover my submitted algorithm and its implementations. As for patent(s) and patent application(s) held by myself, I ☐ have submitted / ☐ have not submitted all statements; as for patent(s) and patent application(s) held by others, I ☐ have submitted / ☐ have not submitted all statements signed by patent and patent application owner(s).

Table The List of Patent(s) and Patent Application(s)

No.	Patent/Patent Application No.	Title of Patent/Patent Application	Patent/Patent Application Owner(s)	Whether submit statements signed by each owner
1				☐ Yes ☐ No
2				☐ Yes ☐ No

Note: The algorithm submitter(s) shall fill in the table according to his/her/their situation.

I do hereby declare that to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my submitted algorithm and its implementations. I commit that to the best of my knowledge, my submitted algorithm and its implementations are in compliance with the laws and regulations of China and other countries, and do not infringe upon legitimate rights and interests of any third party. Where there is a dispute concerning patent infringement or violation of laws and regulations, I commit that the algorithm submitter(s) shall take the responsibility of dealing with it and eliminating negative effects as well as bearing corresponding legal liabilities.

I am fully aware that I bear the legal consequences of this statement.

Signed:  薛润泽

Date: 2026-6-2

(Note: If there are multiple algorithm submitters, the statements shall be signed by each and every one of them.)

B.1 Statement by Each Algorithm Submitter

I, Yamin Liu (full name), No. 156 Bei Qing Road, Haidian District, Beijing, China (full postal address), to the best of my knowledge of my submitted algorithm CreTAKE (name of algorithm) and its implementations (reference and optimized implementations included), do hereby declare:

1. I commit that my submitted algorithm and its implementations are in compliance with the security requirements, including but not limited to the requirements that the algorithm does not contain any backdoor or defect artificially designed and its implementations do not contain any malicious code. I do hereby commit that to the best of my knowledge, my submitted algorithm and its implementations do not contain any data, information or technology that may infringe upon trade secrets, or may involve confidentiality required by the laws and regulations of China and other countries.
2. I acknowledge and agree that my submitted algorithm and its implementations will be provided to the public for evaluation, analysis and review. I agree that any interested party, including the program organizer, public reviewers, etc., can freely use the algorithm and its implementations for evaluation purpose. I acknowledge that the program organizer will select several algorithms as candidates for the next-round evaluation or the finalists after evaluation and analysis; my submitted algorithm might not be selected as a candidate for the next-round evaluation or the finalist. I acknowledge that I will not receive financial or other compensation from the program organizer for my submitted algorithm.
3. To facilitate the next-generation commercial cryptographic algorithm standardization, I acknowledge and agree that if my submitted algorithm is selected for the finalists, the program organizer may modify the algorithm and its implementations out of security, availability or other considerations. If my submitted algorithm is selected for the finalists and to be standardized, I commit to place no restriction on the worldwide disclosure and free adoption of algorithm and its implementations.
4. I commit that the algorithm and its implementations are my (or my team's) own original work. The implementations of my submitted algorithm ☐ do / ☒ do not adopt code or code libraries requiring authorization by third parties. Except those clearly identified, citations and acknowledgment, all the opinions, words, diagrams and data in the submission are my own (or my team's) original research results, and the submission does not contain any published work from other individual or team.
5. (Please check one of the following two options.)
 - ☒ I do not hold and do not intend to hold any patent or patent application which may cover my submitted algorithm and its implementations, and to the best of my knowledge, no patent or patent application may cover my submitted algorithm and its implementations.

- ☐ The following patent(s) and patent application(s) may cover my submitted algorithm and its implementations. As for patent(s) and patent application(s) held by myself, I ☐ have submitted / ☐ have not submitted all statements; as for patent(s) and patent application(s) held by others, I ☐ have submitted / ☐ have not submitted all statements signed by patent and patent application owner(s).

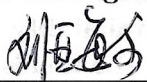
Table The List of Patent(s) and Patent Application(s)

No.	Patent/Patent Application No.	Title of Patent/Patent Application	Patent/Patent Application Owner(s)	Whether submit statements signed by each owner
1				☐ Yes ☐ No
2				☐ Yes ☐ No

Note: The algorithm submitter(s) shall fill in the table according to his/her/their situation.

I do hereby declare that to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my submitted algorithm and its implementations. I commit that to the best of my knowledge, my submitted algorithm and its implementations are in compliance with the laws and regulations of China and other countries, and do not infringe upon legitimate rights and interests of any third party. Where there is a dispute concerning patent infringement or violation of laws and regulations, I commit that the algorithm submitter(s) shall take the responsibility of dealing with it and eliminating negative effects as well as bearing corresponding legal liabilities.

I am fully aware that I bear the legal consequences of this statement.

Signed: Liu Yamin 

Date: 2026-06-02

(Note: If there are multiple algorithm submitters, the statements shall be signed by each and every one of them.)

B.1 Statement by Each Algorithm Submitter

I, Jiabo Wang (full name), No. 19 Shucun Road, Haidian District, Beijing, China (full postal address), to the best of my knowledge of my submitted algorithm CreTAKE (name of algorithm) and its implementations (reference and optimized implementations included), do hereby declare:

1. I commit that my submitted algorithm and its implementations are in compliance with the security requirements, including but not limited to the requirements that the algorithm does not contain any backdoor or defect artificially designed and its implementations do not contain any malicious code. I do hereby commit that to the best of my knowledge, my submitted algorithm and its implementations do not contain any data, information or technology that may infringe upon trade secrets, or may involve confidentiality required by the laws and regulations of China and other countries.
2. I acknowledge and agree that my submitted algorithm and its implementations will be provided to the public for evaluation, analysis and review. I agree that any interested party, including the program organizer, public reviewers, etc., can freely use the algorithm and its implementations for evaluation purpose. I acknowledge that the program organizer will select several algorithms as candidates for the next-round evaluation or the finalists after evaluation and analysis; my submitted algorithm might not be selected as a candidate for the next-round evaluation or the finalist. I acknowledge that I will not receive financial or other compensation from the program organizer for my submitted algorithm.
3. To facilitate the next-generation commercial cryptographic algorithm standardization, I acknowledge and agree that if my submitted algorithm is selected for the finalists, the program organizer may modify the algorithm and its implementations out of security, availability or other considerations. If my submitted algorithm is selected for the finalists and to be standardized, I commit to place no restriction on the worldwide disclosure and free adoption of algorithm and its implementations.
4. I commit that the algorithm and its implementations are my (or my team's) own original work. The implementations of my submitted algorithm ☐ do / ☒ do not adopt code or code libraries requiring authorization by third parties. Except those clearly identified, citations and acknowledgment, all the opinions, words, diagrams and data in the submission are my own (or my team's) original research results, and the submission does not contain any published work from other individual or team.
5. (Please check one of the following two options.)
 - ☒ I do not hold and do not intend to hold any patent or patent application which may cover my submitted algorithm and its implementations, and to the best of my knowledge, no patent or patent application may cover my submitted algorithm and its implementations.

- ☐ The following patent(s) and patent application(s) may cover my submitted algorithm and its implementations. As for patent(s) and patent application(s) held by myself, I ☐ have submitted / ☐ have not submitted all statements; as for patent(s) and patent application(s) held by others, I ☐ have submitted / ☐ have not submitted all statements signed by patent and patent application owner(s).

Table The List of Patent(s) and Patent Application(s)

No.	Patent/Patent Application No.	Title of Patent/Patent Application	Patent/Patent Application Owner(s)	Whether submit statements signed by each owner
1				☐ Yes ☐ No
2				☐ Yes ☐ No

Note: The algorithm submitter(s) shall fill in the table according to his/her/their situation.

I do hereby declare that to the best of my knowledge, I have fully disclosed all patents and patent applications which may cover my submitted algorithm and its implementations. I commit that to the best of my knowledge, my submitted algorithm and its implementations are in compliance with the laws and regulations of China and other countries, and do not infringe upon legitimate rights and interests of any third party. Where there is a dispute concerning patent infringement or violation of laws and regulations, I commit that the algorithm submitter(s) shall take the responsibility of dealing with it and eliminating negative effects as well as bearing corresponding legal liabilities.

I am fully aware that I bear the legal consequences of this statement.

Signed: Jiahao Wang 王嘉豪

Date: 2026-6-2

(Note: If there are multiple algorithm submitters, the statements shall be signed by each and every one of them.)

B.2 Statement by Patent (and Patent Application) Owner(s)

(Please check one of the following two options.)

- ☒ I, Institute of Information Engineering, CAS, No. 19 Shucun Road,
Haidian District, Beijing, China, 100085, am the owner of the patent/patent
application 202510447608.7 (patent number/patent application number);
- ☐ I, _____ (full name), _____ (full postal
address), am the authorized representative of the owner _____
(full name) of the patent/patent application _____ (patent
number/patent application number),

and do hereby agree to grant to any interested party, including the program organizer, public reviewers, etc., the right to freely use the above patent (and patent application) for evaluation purpose, and commit to grant to any interested party, including standard drafter, standard organization department, standard users, etc., a public, irrevocable, nonexclusive, royalty-free license for using the patent (and patent application) without any conditions, if the algorithm CreTAKE (name of algorithm) is selected for standardization.

Signed: _____

Date: _____

(Note: If there are multiple owners of the patent (and patent application), the statements shall be signed by each and every one of them or their authorized representatives. The authorized representative shall submit the letter of authorization.)

B.3 Statement by Reference and Optimized Implementations' Owner(s)

(Please check one of the following two options.)

- ☒ I, Jingnan He (full name), No. 19 Shucun Road, Haidian District, Beijing, China (full postal address), am the owner of the submitted reference implementation and optimized implementations of the algorithm CreTAKE (name of algorithm);
- ☐ I, _____ (full name), _____ (full postal address), am the authorized representative of the owner _____ (full name) of the submitted reference implementation and optimized implementations of the algorithm _____ (name of algorithm),

and do hereby agree that any interested party, including the program organizer, public reviewers, etc., can freely use such implementations for evaluation purpose, and commit to place no restriction on worldwide disclosure and free adoption if the algorithm is selected for standardization.

Signed: Jingnan He 贺婧楠

Date: 2026.6.2

(Note: If there are multiple owners of the reference and optimized implementations, the statements shall be signed by each and every one of them or their authorized representatives. The authorized representative shall submit the letter of authorization.)