WHAT IS CLAIMED IS:

1. A method of identifying quantum vulnerability with respect to an application by using a computing apparatus, the method comprising:

identifying one or more cryptographic associated functions performed in an application based on analysis of a code, executed while the application is in an operating state, by using a dynamic analysis agent corresponding to the application;

based on the one or more cryptographic associated functions, calculating a cryptography algorithm list used in the application; and

based on the cryptography algorithm list, identifying quantum vulnerability with respect to the application;

wherein:

in the calculating, the dynamic analysis agent calculates the cryptography algorithm list used for the application while calling and executing an API of the one or more cryptographic associated functions.

2. The method of claim 1, further comprising correcting, by using the dynamic analysis agent, a code area corresponding to the quantum vulnerability identified in the application that is in the operating state.

3. The method of claim 1, wherein the dynamic analysis agent is configured to identify quantum vulnerability with respect to the application by using a rule set configured based on a predetermined configuration file for the application.

4. The method of claim 1, wherein the application and the dynamic analysis agent are configured to interoperate with each other in one same process.

5. The method of claim 4, wherein the dynamic analysis agent is configured to identify quantum vulnerability with respect to the application that is in the operating state by using intercepting for the application.

6. The method of claim 2, wherein the corrected code area is applied to the application, and

wherein configuration is made not to recall the dynamic analysis agent when the application is recalled.

7. The method of claim 2, wherein a degree of effect on the application is verified by using a code to which the corrected code area is applied.

8. A server comprising a processor and a memory, and configured to identify quantum vulnerability with respect to an application,

wherein the memory comprises instructions configured to cause, when executed by the processor, the server to perform a predetermined operation comprising:

identifying one or more cryptographic associated functions executed in the application based on analysis of a code, executed while the application is in an operating state, by using a dynamic analysis agent corresponding to the application;

calculating, based on the one or more cryptographic associated functions, a cryptography algorithm list used in the application; and

identifying, based on the cryptography algorithm list, the quantum vulnerability with respect to the application;

wherein:

in the calculating, the dynamic analysis agent calculates the cryptography algorithm list used for the application while calling and executing an API of the one or more cryptographic associated functions.

9. The server of claim 8, wherein the predetermined operation further comprises correcting, by using the dynamic

analysis agent, a code area corresponding to the quantum vulnerability identified in the application that is in the operating state.

10. The server of claim 8, wherein the dynamic analysis agent is configured to identify the quantum vulnerability with respect to the application by using a rule set configured based on a predetermined configuration file for the application.

11. The server of claim 8, wherein the application and the dynamic analysis agent are configured to interoperate with each other in one same process.

12. The server of claim 11, wherein the dynamic analysis agent is configured to identify the quantum vulnerability with respect to the application that is in the operating state, by using intercepting for the application.

13. The server of claim 9, wherein the corrected code area is applied to the application, and

wherein configuration is made so as not to recall the dynamic analysis agent when the application is recalled.

14. The server of claim 9, wherein a degree of effect on the application is verified using a code to which the corrected code area is applied.

15. A computer-readable storing medium that stores instructions configured to, when executed by a processor, cause a server to implement a predetermined operation, the server including the processor and identifying quantum vulnerability with respect to an application, and the predetermined operation comprising:

identifying one or more cryptographic associated functions executed in the application based on analysis of a code, executed when the application is in an operating state, by using a dynamic analysis agent corresponding to the application;

based on the one or more cryptographic associated functions, calculating a cryptography algorithm list used in the application; and

based on the cryptography algorithm list, identifying quantum vulnerability with respect to the application;

wherein:

the dynamic analysis agent calculates the cryptography algorithm list used for the application while calling and executing an API of the one or more cryptographic associated functions.