signatures against quantum-capable adversaries. Furthermore, other desirable features and characteristics will become apparent from the subsequent detailed description and the appended claims, taken in conjunction with the accompanying drawings and this background of the disclosure.

SUMMARY

[0007] According to at least one aspect of the present embodiments, a quantum resistant digital signature system is provided. The quantum resistant digital signature system includes a digital signature system and a layer of quantum resistant protection. The digital signature system includes a public key and a private key, wherein the public key is associated with the private key. The digital signature system also includes a digital signature generated in response to data and the private key, wherein computation of the private key is a collapsing hash function. The layer of quantum resistant protection is applied to the digital signature system and includes a signing-party-provided quantum-secure zero-knowledge proof of knowledge. The signing-party-provided quantum-secure zero-knowledge proof of knowledge comprises a zero-knowledge proof of the computation of the private key, zero-knowledge proof of the computation of the public key, and zero-knowledge proof of the computation of the digital signature starting from a pre-image of the private key.

[0008] According to another aspect of the present embodiments, a method for quantum-resistant digitally signing data is provided. The method generating a pre-image parameter in response to a security parameter and generating a private key using a collapsing hash function, wherein the private key is generated in response to the pre-image parameter. The method further includes generating a public key in response to the security parameter, wherein

the public key is generated from the private key. The method further includes generating a signature in response to the data and the private key, generating a zero-knowledge proof of knowledge, and digitally signing the data with both the signature and the zero-knowledge proof of knowledge. The zero-knowledge proof of knowledge comprises a zero-knowledge proof of the computation of the private key, zero-knowledge proof of the computation of the public key, and zero-knowledge proof of the computation of the digital signature starting from a pre-image of the private key.

[0009] According to a further aspect of the present embodiments, a method for verification of a quantum resistant digital signature for authentication of a source of

data by verifying a private key is provided. The private key is generated using a collapsing hash function. The method includes authenticating the source of the data by using: i) a public key associated with the private key, and ii) a zero-knowledge proof of knowledge to verify a digital signature corresponding to the data is generated in response to the private key. The zero-knowledge proof of knowledge comprises a zero-knowledge proof of the computation of the private key, zero-knowledge proof of the computation of the public key, and zero-knowledge proof of the computation of the digital signature starting from a pre-image of the private key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views and which together with the detailed description below are incorporated in and form part of the specification, serve to illustrate various embodiments and to explain various principles and advantages in accordance with present embodiments.

[0011] FIG. 1 depicts an exemplary quantum-resistant ECDSA key generation algorithm $KeyGen_q$ in accordance with the present embodiments.

[0012] FIG. 2 depicts an exemplary quantum-resistant ECDSA signing algorithm $Sign_q$ in accordance with the present embodiments.

[0013] FIG. 3 depicts an exemplary quantum-resistant ECDSA verification algorithm $Verify_q$ in accordance with the present embodiments.

[0014] FIG. 4 depicts a process diagram illustrating use-cases of a real-life implementation of the quantum-resistant digital signature scheme in accordance with the present embodiments under test.

[0015] FIG. 5 depicts images of windows exemplifying the predefined certificate hierarchy in the real-life implementation of the quantum-resistant digital signature scheme in accordance with the present embodiments.

CLAIMS

What is claimed is:

1. A quantum resistant digital signature system comprising:

a digital signature system comprising a public key and a private key, wherein the public key is associated with the private key, wherein the digital signature system comprises a digital signature generated in response to data and the private key, wherein computation of the private key is a collapsing hash function; and

a layer of quantum resistant protection applied to the digital signature system, the layer of quantum resistant protection comprising a signing-party-provided quantum-secure zero-knowledge proof of knowledge,

wherein the signing-party-provided quantum-secure zero-knowledge proof of knowledge comprises a zero-knowledge proof of the computation of the private key, zero-knowledge proof of the computation of the public key, and zero-knowledge proof of the computation of the digital signature starting from a pre-image of the private key.

2. The quantum resistant digital signature system in accordance with Claim 1 wherein a cryptographic key of a predetermined strength generates both the public key and the private key.

3. The quantum resistant digital signature system in accordance with Claim 1 or 2 wherein the signing-party-provided quantum-secure zero-knowledge proof of knowledge is generated in response to at least a portion of the private key.

4. The quantum resistant digital signature system in accordance with any of Claims 1 to 3 wherein the layer of quantum resistant protection supports more than one party by providing a plurality of proofs of knowledge of the pre-image of the private key, the plurality of proofs of knowledge of the pre-image of the private key having a predefined certificate hierarchy.

5. A method for quantum-resistant digitally signing data comprising:

generating a pre-image parameter in response to a security parameter;

generating a private key using a collapsing hash function, wherein the private key is generated in response to the pre-image parameter;

generating a public key in response to the security parameter, wherein the public key is generated from the private key;

generating a signature in response to the data and the private key;

generating a zero-knowledge proof of knowledge ; and

digitally signing the data with both the signature and the zero-knowledge proof of knowledge ,

wherein the zero-knowledge proof of knowledge comprises a zero-knowledge proof of the computation of the private key, zero-knowledge proof of the computation of the public key, and zero-knowledge proof of the computation of the digital signature starting from a pre-image of the private key.

6. The method in accordance with Claim 5 wherein digitally signing the data comprises storing the signature separately from the zero-knowledge proof for parallel verification.

7. The method in accordance with Claim 5 or 6 wherein the security parameter defines a cryptographic key of a predetermined strength.

8. The method in accordance with any of Claims 5 to 7 wherein the zero-knowledge proof of knowledge is generated in response to at least a portion of the private key.

9. The method in accordance with any of Claims 5 to 8 wherein generating the private key comprises one or more of generating the private key by performing a hash key derivation on the pre-image parameter, performing a one-way function key derivation on the pre-image parameter, or performing a symmetric key derivation on the pre-image parameter.

10. The method in accordance with any of Claims 5 to 9 wherein generating the public key and the pre-image parameter comprises one or more of generating the public key by performing a hash key derivation on the pre-image parameter, generating the public key by performing a one-way function key derivation on the pre-image parameter, or generating the public key by performing a symmetric key derivation on the pre-image parameter.

11. The method in accordance with any of Claims 5 to 10 wherein the data comprises a message, the method further comprising sending the digitally signed message, wherein the zero-knowledge proof of knowledge is accessible by a recipient of the message.

12. The method in accordance with Claim 11 wherein sending the digitally signed message comprises sending the digitally signed message along with one or both of (i) the zero-knowledge proof of knowledge or (ii) location information for identifying a digital storage location from which the zero-knowledge proof of knowledge can be accessed.

13. The method in accordance with Claim 11 or Claim 12 further comprising sending the public key, wherein sending the public key comprises sending the digitally signed message along with the public key or sending the public key to a digital storage location, the digital storage location comprising a certification authority or a public repository.

14. A method for verification of a quantum resistant digital signature for authentication of a source of data by verifying a private key, the private key generated using a collapsing hash function, the method comprising:

authenticating the source of the data by using:

i) a public key associated with the private key, and

ii) a zero-knowledge proof of knowledge ,

to verify a digital signature corresponding to the data is generated in response to the private key,

wherein the zero-knowledge proof of knowledge comprises a zero-knowledge proof of the computation of the private key, zero-knowledge proof of the computation of the public key, and zero-knowledge proof of the computation of the digital signature starting from a pre-image of the private key.

15. The method in accordance with Claim 14 wherein the authentication step comprises parallelly processing verification using the public key and verification using the zero-knowledge proof of knowledge.

16. The method in accordance with Claim 15 wherein parallelly processing verification using the public key and verification using the zero-knowledge proof of knowledge comprises:

retrieving the public key from a first digital storage location; and

retrieving the zero-knowledge proof of knowledge from a second digital storage location.

17. The method in accordance with Claims 14 to 16 wherein authenticating the source of the data comprises accepting verification of the data if and only if both the digital signature is determined to be generated in response to the private key and the zero-knowledge proof of knowledge is determined to be a valid proof computed from the pre-image parameter.