

CLAIMS

1. A system comprising:
 - a first node having a key generator configured to generate at least one physical unclonable function (PUF); and
 - 5 a second node configured to remotely send an attestation request to the first node, wherein the first node is configured to respond to the attestation request as part of a verification to join the network.
2. The system of claim 1, wherein the second node is part of a distributed ledger.
3. The system of claim 2, wherein the first node is part of the distributed ledger.
- 10 4. The system of claim 3, wherein a public-private key pair is generated for the first node, wherein the private key is generated for the first node via the at least one PUF, and the public key is registered with the distributed ledger.
5. The system of claim 4, wherein the public key is encrypted before registration with the distributed ledger.
- 15 6. The system of claim 5, wherein the security of the first node is verified through the remote attestation of the public key on the distributed ledger.
7. The system of any one of the preceding claims, wherein the key generator comprises a neuromorphic computing platform.
8. The system of claim 7, wherein the neuromorphic computing platform includes
20 an array of resistive random-access memory (ReRAM).
9. The system of claim 8, wherein the array of ReRAM is arranged in a crossbar array format.
10. The system of claim 9, wherein the crossbar array is a multi-layer crossbar array.
- 25 11. The system of claim 1, wherein the key generator includes at least one of a silicon-based PUF, an electronic PUF, an optical PUF, and a biological PUF.

12. The system of claim 7, wherein the neuromorphic computing platform is installed with an artificial intelligent (AI) based tool, the AI based tool operable to remove the first node if the first node fails the attestation request.

13. The system according to any one of the preceding claims, wherein the system
5 comprises an IoT system.

14. A method for providing security to a system having a first node and a second node, comprising the steps of: -

(a.) generating, via a key generator on the first node, at least one physical unclonable function (PUF);

10 (b.) sending remotely, via the second node, an attestation request to the first node; and

(c.) responding to the attestation request by the first node.

15 15. The method of claim 14, further comprises the step of generating a public-private key pair for the first node, wherein the private key is generated for the first node via the at least one PUF, and the public key is registered with a distributed ledger.

16. The method of claim 14 or 15, wherein the key generator comprises a neuromorphic computing platform.

17. The method of claim 16, wherein the neuromorphic computing platform includes
20 an array of resistive random-access memory (ReRAM).

18. The method of claim 17, wherein the array of ReRAM is arranged in a crossbar array format.

19. The method of claim 18, wherein the crossbar array is a multi-layer crossbar array.

25 20. The method of claim 14, wherein the key generator includes at least one of a silicon-based PUF, an electronic PUF, an optical PUF, and a biological PUF.

21. A device for providing information security comprising:

a secured microkernel; and

a key generator configured to generate at least one physical unclonable function (PUF), wherein the at least one key generator is configured to generate a public-private key pair.

5