

What is claimed is:

1. An authenticatable device for use with an authentication system, comprising:
  - a. a physically-unclonable function ('PUF') device having a PUF input and a PUF output and constructed so as to, in response to the input of a specific challenge C, generate an output O that is characteristic to the PUF and the specific challenge C;
  - b. a processor having a processor input that is connected to the PUF output, the processor configured to:
    - i. in response to the receipt of an output O from the PUF output, generate a commitment value that depends upon a private value r; and
    - ii. in response to the contemporaneous receipt of an authentication query that includes a nonce and of an output O from the PUF output, return a zero knowledge proof authentication value that corresponds to the commitment value;wherein the zero knowledge proof authentication value further corresponds to an authentication token that includes a blinded value that depends upon the private value r and a random value, and wherein the processor is configured to decrypt the random value.
2. The authenticatable device of claim 1, wherein the authentication system has a working verification set that includes the specific challenge C and commitment value.

3. The authenticatable device of claim 2, wherein the authentication system has a limited verification set that includes the specific challenge C and a corresponding token.
4. The authenticatable device of claim 1, wherein the authentication system includes: a root server having a working verification set that includes the specific challenge C and commitment value; and a child server having a limited verification set that includes the specific challenge C and a corresponding token.
5. The authenticatable device of claim 1, wherein the authentication system includes: a root server having a working verification set that includes the specific challenge C and commitment value; and a plurality of child servers each having a different limited verification set; wherein each limited verification set includes the specific challenge C and a corresponding token that is specific to the particular child server.
6. An authenticatable device for use with an authentication system that includes a root server having a working verification set and a child server having a limited verification set, the authenticatable device comprising:
  - a. a physically-unclonable function ('PUF') device having a PUF input and a PUF output and constructed so as to, in response to the input of a specific challenge C, generate an output O that

is characteristic to the PUF and the specific challenge C;

- b. a processor having a processor input that is connected to the PUF output, the processor configured to:
  - i. in response to the receipt of an output O from the PUF output, generate a commitment value that depends upon a private value r; and
  - ii. in response to the contemporaneous receipt of an authentication query that includes a nonce and of an output O from the PUF output, return a zero knowledge proof authentication value that corresponds to the commitment value;

wherein the working verification set includes the specific challenge C and commitment value and the limited verification set includes the specific challenge C and a corresponding derived token that includes a blinded value that depends upon the private value r blinded with a random value, wherein the zero knowledge proof authentication value further corresponds to the derived token, and wherein the processor is configured to decrypt the random value.

- 7. The authenticatable device of claims 1 or 6, wherein the random value is generated externally from the authenticatable device and the processor is configured to decrypt the random value using a key.
- 8. The authenticatable device of claims 1 or 6, wherein the processor is configured to, during generation of

the commitment value, generate and discard the private value  $r$ .

9. The authenticatable device of claims 1 or 6, wherein the commitment value is an exponential function of the private value  $r$ .
10. The authenticatable device of claims 1 or 6, wherein the blinded value depends exponentially upon the private value  $r$  multiplied by the random value.
11. The authenticatable device of claims 1 or 6, wherein the commitment value is an exponential function of the private value  $r$  and wherein the blinded value depends exponentially upon the private value  $r$  multiplied by the random value.
12. The authenticatable device of claims 1 or 6, wherein the random value is an element of a group of prime order.
13. The authenticatable device of claims 1 or 6, wherein the PUF device is a controlled PUF device.
14. The authenticatable device of claims 1 or 6, wherein the PUF device is a super high information content PUF.
15. The authenticatable device of claims 1 or 6, wherein the processor is further configured to perform operations as part of an extended Boyko-Peinado-Venkatesan generation.

16. An authenticatable device for use with an authentication entity, comprising:
- a. a physically-unclonable function ('PUF') device having a PUF input and a PUF output and constructed so as to, in response to the input of a specific challenge C, generate an output O that is characteristic to the PUF and the specific challenge C;
  - b. a processor having a processor input that is connected to the PUF output and connectable to the authentication entity and a processor output that is connectable to the authentication entity, the processor configured to:
    - i. in response to the receipt of an output O from the PUF output, generate a commitment value that depends upon a private value r; and
    - ii. in response to the contemporaneous receipt of an authentication query that includes a nonce and of an output O from the PUF output, perform operations as part of an extended Boyko-Peinado-Venkatesan generation and return a zero knowledge proof authentication value that corresponds to the commitment value.
17. The authenticatable device of claim 16, wherein the processor is further configured to receive pre-processed exponents from the authentication server and employ those exponents in extended Boyko-Peinado-Venkatesan generation.

18. The authenticatable device of claim 16, wherein the processor is further configured to perform operations including the input and processing of a hash chain.
19. The authenticatable device of claims 1, 6, or 16, wherein the processor is further configured to, in response to the receipt of an output O from the PUF output, generate a helper string along with the commitment value.
20. An authenticatable device for use with an authentication entity, comprising:
  - a. a physically-unclonable function ('PUF') device having a PUF input and a PUF output and constructed so as to, in response to the input of a specific challenge C, generate an output O that is characteristic to the PUF and the specific challenge C;
  - b. a processor having a processor input that is connected to the PUF output and connectable to the authentication entity and a processor output that is connectable to the authentication entity, the processor configured to:
    - i. in response to the receipt of an output O from the PUF output, generate a commitment value and a helper string that depend upon a private value r; and
    - ii. in response to the contemporaneous receipt of an authentication query and of an output O from the PUF output, generate a full block value based on the output O, break the full

block value into a plurality of subparts, carry out error-correcting code on each of the subparts, and return a zero knowledge proof authentication value that corresponds to the commitment value.

21. The authenticatable device of claim 20, wherein the error-correcting code is Bose-Chaudhuri-Hocquenghem ('BCH') code.
22. The authenticatable device of claims 16 or 20, wherein the authenticatable device is resource-constrained.
23. The authenticatable device of claims 16 or 20, wherein the authenticatable device is a mobile device.
24. An authenticatable device for use with an authentication system, comprising:
  - a. an internal input and an internal output constructed so as to, in response to the internal input of a specific challenge C, generate an internal output O that is characteristic to the device and the specific challenge C;
  - b. a processor having a processor input that is connected to the internal output, the processor configured to:
    - i. in response to the receipt of an output O from the internal output, generate a commitment value that depends upon the output O and a private value r; and

ii. in response to the contemporaneous receipt of an authentication query that includes a nonce and of an output O from the internal output, return a zero knowledge proof authentication value that corresponds to the commitment value;

wherein the zero knowledge proof authentication value further corresponds to an authentication token that includes a blinded value that depends upon the private value r and a random value, and wherein the processor is configured to decrypt the random value.

25. The authenticatable device of claim 24, further comprising a physically-unclonable function ('PUF') having a PUF input and a PUF output, wherein the PUF input is the internal input and the PUF output is the internal output, and wherein the output O is characteristic to the PUF.

26. The authenticatable device of claim 25, wherein the dependency of the commitment value upon the output O consists of a dependency upon an error-correction helper string.

27. The authenticatable device of claim 24, further comprising a field-programmable gate array ('FPGA'), wherein the PUF resides in the FPGA.

28. The authenticatable device of claim 27, wherein the FPGA is part of a Spartan®-6 FPGA SP605 development board.

29. An authentication system for use with an authenticatable device that is constructed so as to, in response to the input of a specific challenge C, internally generate an output O that is characteristic to the device and the specific challenge C, and that is configured to: i) upon receiving the specific challenge C, generate a corresponding commitment value that depends upon the output O and a private value r, and ii) upon receiving an authentication query that includes the specific challenge C and a nonce, return a zero knowledge proof authentication value that corresponds to the commitment value; the authentication system comprising an enrollment server that:
- a. has a working verification set that includes the specific challenge C and the authenticatable device's corresponding commitment value; and
  - b. is configured to generate an authentication token that:
    - i. includes a blinded value that depends upon the private value r and a random value that can be decrypted by the authenticatable device; and
    - ii. corresponds to the zero knowledge proof authentication value.
30. The authentication system of claim 29, wherein the enrollment server is configured to generate the random value.
31. The authentication system of claim 29, wherein the enrollment server is configured to encrypt the random

value with a key that is shared with the authenticatable device.

32. The authentication system of claim 29, wherein the commitment value is an exponential function of the private value  $r$ .
33. The authentication system of claim 29, wherein the blinded value depends exponentially upon the private value  $r$  multiplied by the random value.
34. The authentication system of claim 29, wherein the commitment value is an exponential function of the private value  $r$  and wherein the blinded value depends exponentially upon the private value  $r$  multiplied by the random value.
35. The authentication system of claim 29, wherein the random value is an element of a group of prime order.
36. The authentication system of claim 29, wherein the enrollment server is configured to generate a limited verification set that includes the specific challenge  $C$  and authentication token.
37. The authentication system of claim 36, wherein the limited verification set further includes an error-correction helper string, and the dependency of the commitment value upon the output  $O$  consists of a dependency upon the error-correction helper string.
38. The authentication system of claim 36, further comprising an authentication server having the limited verification set.

39. The authentication system of claim 36, further comprising a plurality of authentication servers each having a different limited verification set, wherein each limited verification set includes the specific challenge C and a corresponding token that is specific to the particular authentication server.
40. The authentication system of claim 29, wherein the enrollment server has a complete verification set that includes multiple different specific challenge values and the authenticatable device's corresponding commitment values.
41. The authentication system of claim 29, wherein the enrollment server possesses challenge values and corresponding commitment values for multiple authenticatable devices.
42. The authentication system of claim 29, wherein the output O of the authenticatable device which the system is for use with is generated by a physically-unclonable function ('PUF') in the authenticatable device.
43. The authentication system of claim 42, wherein the PUF of the authenticatable device which the system is for use with resides in a field-programmable gate array.
44. The authentication system of claim 29, further comprising an authenticatable device having a physically-unclonable function ('PUF') capable of generating the output O.

45. The authentication system of claim 44, wherein the  
PUF resides in a field-programmable gate array.