CLAIMS:

1. A method for accessing a wireless network, the method comprising:

generating, by a first device, a first message of a one-round key exchange protocol;

embedding, by the first device, the first message into a beacon packet and broadcasting the beacon packet such that a second wireless device receives the first message and responds by generating a response message based on the first message;

receiving, by the first device, the response message from the second wireless device, wherein the response message comprises encrypted configuration data and a second message of the one-round key exchange protocol;

computing, by the first device, a shared key K_S using the first message and the second message;

decrypting, by the first device, the encrypted configuration data using the shared key K_S; and

accessing, by the first device, the wireless network using the configuration data

wherein the one-round key exchange protocol comprises a Two-Basis Password Exponential Key Exchange (TBPEKE) protocol,

wherein the first message comprises a first token computed using a shared token G_S and a random value x, the second message comprises a second token computed using the shared token G_S and a random value y, and the shared key K_S is computed using the shared token G_S and the random values x and y, and

whereby the shared token is derived using two fixed points (U, V) on an Elliptic Curve Cryptography (ECC) and a random value w that were pre-loaded in the first and second wireless devices.

2. The method according to claim 1, wherein the response message further comprises a message authentication code (MAC) generated by the second wireless device,

wherein before the step of decrypting the encrypted configuration data using the shared key K_S, the method further comprises:

verifying the MAC using the computed shared key K_S; and

wherein the step of decrypting the encrypted configuration data using the shared key K_S comprises:

decrypting the encrypted configuration data using the shared key K_S in response to verifying the MAC.

3. The method according to claim 1, wherein the first token is computed by multiplying the shared token G_S with the random value x, the second token is computed by multiplying the shared token G_S with the random value y, the shared key K_S is computed by multiplying the shared token G_S with the random values x and y, and the shared token G_S is derived by:

$$G_S = U + w \cdot V.$$

4. The method according to claim 1,

wherein the one-round key exchange protocol comprises an Elliptic Curve Diffie-Hellman (ECDH) protocol,

wherein the first message comprises a first public key computed using a first private key and a finite cyclic group G, the second key comprises a second public key computed using a second private key and the finite cyclic group G, and the shared key K_S is computed using the first private key, the second private key and the finite cyclic group G, and

whereby the finite cyclic group G is pre-loaded in the first and second wireless devices.

5. The method according to claim 4, wherein the first public key is computed by multiplying the first private key with the finite cyclic group G, the second public key is computed by multiplying the second private key with the finite cyclic group G, and the shared key K_S is computed by multiplying the first private key with the second private key and the finite cyclic group G.

6. A first wireless device, comprising:

a processor; and

a memory readable by the processor, the memory storing instructions that when executed by the processor, cause the processor to:

generate a first message of a one-round key exchange protocol;

embed the first message into a beacon packet and broadcast the beacon packet such that a second wireless device receives the first message and responds by generating a response message based on the first message;

receive the response message from the second wireless device, wherein the response message comprises encrypted configuration data and a second message of the one-round key exchange protocol;

compute a shared key K_S using the first message and the second message;

decrypt the encrypted configuration data using the shared key K_S; and

access the wireless network using the configuration data

wherein the one-round key exchange protocol comprises a Two-Basis Password Exponential Key Exchange (TBPEKE) protocol,

wherein the first message comprises a first token computed using a shared token G_S and a random value x, the second message comprises a second token computed using the shared token G_S and a random value y, and the shared key K_S is computed using the shared token G_S and the random values x and y, and

whereby the shared token is derived using two fixed points (U, V) on an Elliptic Curve Cryptography (ECC) and a random value w that were pre-loaded in the first and second wireless devices.

7. The first wireless device according to claim 6, wherein the response message further comprises a message authentication code (MAC) generated by the second wireless device,

wherein before the instructions direct the processor to decrypt the encrypted configuration data using the shared key K_S, the instructions direct the processor to:

verify the MAC using the computed shared key K_S; and

wherein decrypting the encrypted configuration data using the shared key K_S comprises:

decrypting the encrypted configuration data using the shared key K_S in response to verifying the MAC.

8. The first wireless device according to claim 6, wherein the first token is computed by multiplying the shared token G_S with the random value x, the second token is computed by multiplying the shared token G_S with the random value y, the shared key K_S is computed by multiplying the shared token G_S with the random values x and y, and the shared token G_S is derived by:

$$G_S = U + w \cdot V.$$

9. The first wireless device according to claim 6,

wherein the one-round key exchange protocol comprises an Elliptic Curve Diffie-Hellman (ECDH) protocol,

wherein the first message comprises a first public key computed using a first private key and a finite cyclic group G, the second key comprises a second public key computed using a second private key and the finite cyclic group G, and the shared key K_S is computed using the first private key, the second private key and the finite cyclic group G, and

whereby the finite cyclic group G is pre-loaded in the first and second wireless devices.

10. The first wireless device according to claim 9, wherein the first public key is computed by multiplying the first private key with the finite cyclic group G, the second public key is computed by multiplying the second private key with the finite cyclic group G, and the shared key KS is computed by multiplying the first private key with the second private key and the finite cyclic group G.

11. A non-transitory computer-readable medium storing instructions that, when executed by a processor in first wireless device, cause the processor to:

generate a first message of a one-round key exchange protocol;

embed the first message into a beacon packet and broadcast the beacon packet such that a second wireless device receives the first message and responds by generating a response message based on the first message;

receive the response message from the second wireless device, wherein the response message comprises encrypted configuration data and a second message of the one-round key exchange protocol;

compute a shared key K_S using the first message and the second message;

decrypt the encrypted configuration data using the shared key K_S; and

access the wireless network using the configuration data

wherein the one-round key exchange protocol comprises a Two-Basis Password Exponential Key Exchange (TBPEKE) protocol,

wherein the first message comprises a first token computed using a shared token G_S and a random value x, the second message comprises a second token computed using the shared token G_S and a random value y, and the shared key K_S is computed using the shared token G_S and the random values x and y, and

whereby the shared token is derived using two fixed points (U, V) on an Elliptic Curve Cryptography (ECC) and a random value w that were pre-loaded in the first and second wireless devices.

12. The computer-readable medium according to claim 11, wherein the response message further comprises a message authentication code (MAC) generated by the second wireless device,

wherein before decrypting the encrypted configuration data using the shared key K_S, the instructions cause the processor to:

verify the MAC using the computed shared key K_S; and

wherein decrypting the encrypted configuration data using the shared key K_S comprises:

decrypting the encrypted configuration data using the shared key K_S in response to verifying the MAC.

13. The computer-readable medium according to claim 11, wherein the first token is computed by multiplying the shared token G_S with the random value x, the second token is computed by multiplying the shared token G_S with the random value y, the shared key K_S is computed by multiplying the shared token G_S with the random values x and y, and the shared token G_S is derived by:

$$G_S = U + w \cdot V.$$

14. The computer-readable medium according to claim 11,

wherein the one-round key exchange protocol comprises an Elliptic Curve Diffie-Hellman (ECDH) protocol,

wherein the first message comprises a first public key computed using a first private key and a finite cyclic group G, the second key comprises a second public key computed using a second private key and the finite cyclic group G, and the shared key K_S is computed using the first private key, the second private key and the finite cyclic group G, and

whereby the finite cyclic group G is pre-loaded in the first and second wireless devices.

15. The computer-readable medium according to claim 14, wherein the first public key is computed by multiplying the first private key with the finite cyclic group G, the second public key is computed by multiplying the second private key with the finite cyclic group G, and the shared key KS is computed by multiplying the first private key with the second private key and the finite cyclic group G.