

words, such as addition, exclusive-or, or a more complex cryptographic function. The cryptographic secret in various embodiments can be used as encryption key, a decryption key, a signature key, or the seed for deriving one or more cryptographic keys. The cryptographic secret in various embodiments can be used in a digital signature algorithm or in an identification algorithm.

[0152] Accordingly, the invention is to be defined not by the preceding illustrative description but instead by the spirit and scope of the following claims.

What is claimed is:

1. A method for establishing a secret to authenticate a user comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices;

converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

selecting a codeword from a plurality of codewords for each value in the sequence of values to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code;

calculating a security value of a security parameter from the sequence of codewords; and

comparing the security value of the security parameter to a threshold value.

2. The method of claim 1 wherein the security parameter is entropy.

3. The method of claim 1 wherein the security parameter is minentropy.

4. The method of claim 1 further comprising the step of rejecting the secret pattern if the security value of the security parameter does not meet or exceed the threshold value.

5. The method of claim 1 further comprising, if the security value of the security parameter meets or exceeds the threshold value, the steps of:

calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets; and

hashing the sequence of codewords to produce a hash of the sequence of codewords.

6. The method of claim 5 further comprising storing the sequence of offsets for use in authenticating a user.

7. The method of claim 6 further comprising storing the hash of the sequence of codewords for use in authenticating a user.

8. The method of claim 6 further comprising transmitting the hash of the sequence of codewords to an authentication device for use in authenticating a user.

9. A method for establishing a secret to authenticate a user comprising the steps of:

receiving a secret pattern on a graphical interface, wherein the secret pattern comprises a sequence of discrete graphical choices;

converting each discrete graphical choice in the sequence of discrete graphical choices into a value to produce a sequence of values, wherein the sequence of values corresponds to the sequence of discrete graphical choices;

selecting a codeword from a plurality of codewords for each value in the sequence of values to generate a sequence of codewords, the plurality of codewords being associated with an error-correcting code;

calculating an offset between each value in the sequence of values and the corresponding codeword in the sequence of codewords to generate a sequence of offsets; and

hashing the sequence of codewords to produce a hash of the sequence of codewords.

10. The method of claim 9 wherein a discrete graphical choice in the sequence of discrete graphical choices comprises a selected point on the graphical interface.

11. The method of claim 10 further comprising the step of displaying an image on the graphical interface after receiving the selected point on the graphical interface, wherein each discrete graphical choice in the sequence of discrete graphical choices is associated with one of a plurality of images.

12. The method of claim 11 further comprising prompting a user by displaying one of the plurality of images on the graphical interface; and receiving a match pattern on the graphical interface for comparison with the secret pattern, wherein the match pattern comprises a sequence of match points.

13. The method of claim 12 further comprising, during or after the step of receiving the match pattern on the graphical interface, displaying the selected point associated with the image on the graphical interface.

14. The method of claim 13 further comprising, during or after the step of receiving the match pattern on the graphical interface, displaying a line from a match point to the selected point associated with the image on the graphical interface.

15. The method of claim 10 further comprising providing at least one memory cue by presenting the at least one memory cue in response to a point on the image on the graphical interface being highlighted.

16. The method of claim 15 further comprising associating a first icon from a plurality of icons with a first point on the image on the graphical interface by displaying the first icon in response to the first point being highlighted; and associating a second icon from the plurality of icons with a second point on the image on the graphical interface by displaying the second icon in response to the second point being highlighted.

17. The method of claim 10 further comprising highlighting, for each discrete graphical choice in the sequence of discrete graphical choices, a plurality of points on the graphical interface as alternative graphical choices.

18. The method of claim 9 further comprising storing the sequence of offsets for use in authenticating a user.

19. The method of claim 9 further comprising storing the hash of the sequence of codewords for use in authenticating a user.