SUMMARY

[0004a] According to a first aspect, there is provided a contactless card including: a memory; at least one communication interface; and one or more processors operable to execute stored instructions that, when executed, cause the one or more processors to: determine whether the at least one communication interface is in a near-field communication (NFC) communication with an NFC reader of a computing device; generate a random number via a secure random number generator; convert the random number into a sequence of one or more human-readable characters, wherein the one or more human-readable characters are alphanumeric characters readable by a user; generate a password based on the one or more human-readable characters, wherein the password is different from the sequence of the one or more human-readable characters, the generated password including alphanumeric characters, wherein the generation of the password includes transforming the one or more human-readable characters by: (i) rearranging or capitalizing at least a portion of the one or more human-readable characters and (ii) adding a predefined number of additional human-readable characters; and transmit the password via the at least one communication interface to the computing device, the transmitted password being a master password for triggering execution of at least one application on the computing device for managing one or more passwords used for accessing at least another application.

[0004b] According to a second aspect, there is provided a method including: determining, via one or more processors of a contactless card, whether at least one communication interface of the contactless card is in a near-field communication (NFC) communication with an NFC reader of a computing device; generating, via a secure random number generator of the contactless card, a random number; converting, via the one or more processors of the contactless card, the random number into a sequence of one or more human-readable characters, wherein the one or more human-readable characters are alphanumeric characters readable by a user; generating, via the one or more processors of the contactless card, a password based on the one or more human-readable characters, wherein the password is different from the sequence of the one or more human-readable characters, the generated password including alphanumeric characters, wherein the generation of the password includes transforming the one or more human-readable characters by: (i) rearranging or capitalizing at least a portion of the one or more human-readable characters and (ii) adding a predefined number of additional human-readable characters; and transmitting, via the at least one communication interface of the contactless card, the password to the computing device, the transmitted password being a master password for triggering execution of at least one

application on the computing device for managing one or more passwords used for accessing at least another application.

[0004c] According to a third aspect, there is provided a non-transitory computer readable storage medium storing computer-readable program code executable by at least one processor to: determine, at a countless card, whether at least one communication interface of the contactless card is in a near-field communication (NFC) communication with an NFC reader of a computing device; generate, at the contactless card, a random number via a secure random number generator; convert, at the contactless card, the random number into a sequence of one or more human-readable characters, wherein the one or more human-readable characters are alphanumeric characters readable by a user; generate, at the contactless card, a password based on the one or more human-readable characters, wherein the password is different from the sequence of the one or more human-readable characters, the generated password including alphanumeric characters, wherein the generation of the password includes transforming the one or more human-readable characters by: (i) rearranging or capitalizing at least a portion of the one or more human-readable characters and (ii) adding a predefined number of additional human-readable characters; and transmit the password via the at least one communication interface of the contactless card to the computing device, the transmitted password being a master password for triggering execution of at least one application on the computing device for managing one or more passwords used for accessing at least another application.

[0005] Various embodiments are directed to securely generating and managing passwords using a near-field communication (NFC) enabled contactless smart card. For example, a secure password may be generated by generating a random number via a random number generator of the contactless smart card and converting the random number to one or more human-readable characters. In another example, a secure cryptographic hash function of the contactless smart card may generate a hash output value, which may be converted to one or more human-readable characters. The human-readable characters may be used as the secure password or it may be transformed to add more layers of security and complexity.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] **FIG. 1A** illustrates an example data transmission system in accordance with one or more embodiments.

[0007] **FIG. 1B** illustrates an example sequence diagram for providing authenticated access in accordance with one or more embodiments.

[0008] **FIG. 2** illustrates an example system using a contactless card in accordance with one or more embodiments.

[0009] **FIG. 3A** illustrates an example contactless card in accordance with one or more embodiments.

[0010] **FIG. 3B** illustrates an example contact pad of a contactless card in accordance with one or more embodiments.

[0011] **FIG. 4** illustrates an example sequence diagram relating to secure password generation in accordance with one or more embodiments.

[0012] **FIG. 5** illustrates an example password manager application and secure password generation in accordance with one or more embodiments.

[0013] **FIG. 6** illustrates another example of a sequence diagram relating to secure password generation in accordance with one or more embodiments.

[0014] **FIG. 7** illustrates an example secure password generation for a website in accordance with one or more embodiments.