

CLAIMS

1. A method of computerized data encryption, comprising:
 - receiving, by a computer, capacitive inputs representing multiple passwords associated with multiple users, each password of the multiple passwords associated with a corresponding user of the multiple users;
 - receiving, by the computer, a first capacitive selection representing a minimum number of the multiple passwords;
 - receiving, by the computer, a second capacitive selection representing an electronic data to encrypt;
 - generating, by the computer, a vault key based on the capacitive inputs representing the multiple passwords and the first capacitive selection representing the minimum number of the multiple passwords; and
 - generating, by the computer, an encrypted version of the electronic data by encrypting the electronic data using the vault key as an encryption parameter to an encryption algorithm.
2. The method of claim 1, further comprising storing the vault key.
3. The method of claim 1, further comprising prompting for the multiple passwords entered by the multiple users.
4. The method of claim 1, further comprising providing the multiple passwords and the minimum number of the multiple passwords to a secret sharing algorithm.
5. The method of claim 1, further comprising receiving an output selection to output a physical version of the vault key.
6. The method of claim 1, further comprising receiving an output selection to output a physical version of the encrypted version of the electronic data.

7. The method of claim 1, further comprising avoiding a cache miss by caching the vault key to a processor cache memory.
8. A system, comprising:
 - a hardware processor; and
 - a memory device storing instructions that when executed by the hardware processor perform operations, the operations comprising:
 - receiving a first selection via a graphical user interface of a number of authorized individuals required for an encryption of an electronic data;
 - receiving multiple passwords entered by the authorized individuals via the graphical user interface, each password of the multiple passwords entered by a corresponding individual of the number of the authorized individuals required for the encryption of the electronic data;
 - receiving a second selection via the graphical user interface representing a minimum number of the multiple passwords that are required for a decryption operation;
 - generating a cryptographic vault key from the multiple passwords entered by the authorized individuals and from the minimum number of the multiple passwords that are required for the decryption; and
 - generating an encrypted version of the electronic data by encrypting the electronic data using the cryptographic vault key derived from the multiple passwords entered by the authorized individuals and from the minimum number of the multiple passwords that are required for the decryption operation.
9. The system of claim 8, wherein the operations further comprise receiving inputs representing the multiple passwords entered by the multiple users.
10. The system of claim 8, wherein the operations further comprise prompting for the multiple passwords entered by the multiple users.

11. The system of claim 8, wherein the operations further comprise providing the multiple passwords and the minimum number of the multiple passwords to a secret sharing algorithm.
12. The system of claim 8, wherein the operations further comprise receiving an output selection to output a physical version of the vault key.
13. The system of claim 8, wherein the operations further comprise receiving an output selection to output a physical version of the encrypted version of the electronic data.
14. The system of claim 8, wherein the operations further comprise storing the vault key.
15. The system of claim 8, wherein the operations further comprise storing the encrypted version of the electronic data.
16. A memory device storing instructions that, when executed by a hardware processor, facilitate performance of operations, the operations comprising:
 - receiving a request via a graphical user interface to execute an encryption operation;
 - prompting via the graphical user interface to input a number N of authorized individuals that are required for an encryption of an electronic data;
 - in response to the prompting to input the number of the authorized individuals, receiving a first selection via the graphical user interface representing the number N of the authorized individuals required for the encryption of the electronic data;
 - prompting via the graphical user interface to input multiple identity credentials;
 - in response to the prompting to input the multiple identity credentials, receiving multiple passwords and multiple biometric inputs, each password of the multiple passwords and each biometric input of the multiple biometric inputs entered by a corresponding individual of the authorized individuals required for the encryption of the electronic data;
 - prompting via the graphical user interface to input a minimum number of the multiple identity credentials that are required for a decryption operation;

in response to the prompting to input the minimum number, receiving a second selection via the graphical user interface representing the minimum number of the multiple identity credentials that are required for the decryption operation;

deriving a cryptographic keypair using the multiple passwords, the multiple biometric inputs, and the minimum number of the multiple identity credentials that are required for the decryption; and

generating an encrypted version of the electronic data by encrypting the electronic data using a key of the cryptographic keypair derived using the multiple passwords, the multiple biometric inputs, and the minimum number of the multiple identity credentials that are required for the decryption.

17. The memory device of claim 16, wherein the operations further comprise providing at least one of the multiple passwords, the multiple biometric inputs, and the minimum number of the multiple identity credentials to a secret sharing algorithm.
18. The memory device of claim 16, wherein the operations further comprise deriving a vault key using the multiple passwords, the multiple biometric inputs, and the minimum number of the multiple identity credentials.
19. The memory device of claim 16, wherein the operations further comprise:
 - receiving another request via a graphical user interface to execute the decryption operation;
 - prompting via the graphical user interface to input the minimum number of the multiple identity credentials that are required for the decryption operation;
 - in response to the prompting to input the minimum number of the multiple identity credentials, receiving inputs via the graphical user interface representing the minimum number of the multiple identity credentials that are required for the decryption operation;
 - deriving a decryption key using the minimum number of the multiple identity credentials that are required for the decryption; and

regenerating the electronic data by decrypting the encrypted version using the decryption key derived using the minimum number of the multiple identity credentials that are required for the decryption.