

CLAIMS

What is claimed is:

1. A system comprising:
at least one processor;
at least one memory communicatively coupled to the at least one processor; and
wherein, when at least one encryption key needs to be generated to encrypt a key, the at least one processor is configured to:
generate the at least one encryption key;
encrypt the key using the at least one encryption key to generate an encrypted key;
split the encrypted key ~~and the at least one encryption key into at least one~~ into a first set of first key components, wherein at least a first subset of the first set of first key components of the at least one set of key components can be used to reconstruct the encrypted key, wherein the first set of first key components are configured to be provided to a first plurality of users; and
split the at least one encryption key into at least a second set of second key components, wherein at least a second subset of the at least the second set of second key components can be used to reconstruct the at least one encryption key, wherein the at least the second set of second key components are configured to be provided to a second plurality of users; and
erase the key from the at least one memory.
2. The system of claim 1, wherein the at least one processor is configured to:
combine the encrypted key and the at least one encryption key together before splitting the encrypted key into the first set of first key components and the at least one encryption key into the at least ~~one~~ the second set of second key components.

3. ~~The system of claim 1, wherein the at least one processor is configured to split the encrypted key and the at least one encryption key into the at least one set of key components at least in part by being configured to:~~

~~—— split the encrypted key into a first set of first key components, wherein at least a first subset of the first set of the first key components can be used to reconstruct the encrypted key, wherein the first set of the first key components are configured to be provided to a first plurality of users; and~~

~~—— split the at least one encryption key into at least a second set of second key components, wherein at least a second subset of the second set of the second key components can be used to reconstruct the at least one encryption key, wherein the at least the second set of the second key components are configured to be provided to a second plurality of users.~~

4. ~~The system of claim 3, wherein the at least the second set of the second key components includes only a single set of key components;~~

~~—— wherein the second plurality of users includes only a single set of users; and~~

~~—— wherein the second set of second key components are configured to be provided to the single set of users.~~

53. The system of claim 13, wherein the at least the second set of the second key components includes a plurality of sets of key components;

wherein the second plurality of users includes a plurality of sets of users; and

wherein each set of key components of the plurality of sets of key components is configured to be provided to a corresponding set of users of the plurality of sets of users.

64. The system of claim 13, further comprising:

at least one network interface communicatively coupled to the at least one processor and configured to communicate with external computing devices, the at least one network interface configured to:

cause the at least one network interface to communicate the first set of the first key components to first external computing devices for the first plurality of users; and

cause the at least one network interface to communicate the at least the second set of ~~the~~ second key components to second external computing devices for the second plurality of users.

75. The system of claim ~~46~~, wherein at least one of the first set of ~~the~~ first key components and the at least the second set of ~~the~~ second key components are communicated to users in at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, push verify notification, polling a notification, pulling a notification, or by Bluetooth, WiFi, or near field (NFC) transmission.

86. The system of claim 1, wherein, when the key needs to be generated, the at least one processor is configured to:

generate the key before encrypting the key using the at least one encryption key to generate the encrypted key.

97. The system of claim 1, wherein the at least one processor is configured to encrypt the key by being configured to apply at least one exclusive or (XOR) operation to the key and the at least one encryption key.

~~108.~~ The system of claim 1, wherein the at least one processor is configured to: (1) split the encrypted key into the first set of first key components through at least one of polynomial interpolation or Shamir secret sharing; and (2) split the at least one encryption key into the at least ~~one~~the second set of second key components through at least one of polynomial interpolation or Shamir secret sharing.

119. A system comprising:

at least one processor;

at least one memory communicatively coupled to the at least one processor;

at least one network interface communicatively coupled to the at least one processor and configured to communicate with external computing devices; and

wherein the at least one processor is configured to:

generate a private key;
generate at least one encryption key;
apply at least one exclusive or (XOR) operation to the private key and the at least one encryption key to encrypt the private key using the at least one encryption key to generate an encrypted private key;

~~split the encrypted private key and the at least one encryption key into at least one into a first set of first key components, wherein at least a first subset of the first set of first key components of the at least one set of key components can be used to reconstruct the encrypted private key, wherein the first set of first key components are configured to be provided to a first plurality of users; and~~

~~split the at least one encryption key into at least a second set of second key components, wherein at least a second subset of the second set of second key components can be used to reconstruct the at least one encryption key, wherein the at least the second set of second key components are configured to be provided to a second plurality of users; and~~

erase the at least one encryption key from the at least one memory.

4210. The system of claim 944, wherein the at least one processor is configured to:

combine the encrypted private key and the at least one encryption key together before splitting the encrypted private key into the first set of first key components and the at least one encryption key into the at least ~~one~~ the second set of second key components.

~~13. The system of claim 11, wherein the at least one processor is configured to split the encrypted private key and the at least one encryption key into the at least one set of key components at least in part by being configured to:~~

~~—— split the encrypted private key into a first set of first key components, wherein at least a first subset of the first set of the first key components can be used to reconstruct the encrypted private key, wherein the first set of the first key components are configured to be provided to a first plurality of users; and~~

~~—— split the at least one encryption key into at least a second set of second key components, wherein at least a second subset of the second set of the second key components can be used to~~

~~reconstruct the at least one encryption key, wherein the at least the second set of the second key components are configured to be provided to a second plurality of users.~~

1411. The system of claim 944, wherein the at least one processor is configured to: (1) split the encrypted private key into the first set of first key components through at least one of polynomial interpolation or Shamir secret sharing; and (2) split the at least one encryption key into the at least one the second set of second key components through at least one of polynomial interpolation or Shamir secret sharing.

1512. A system comprising:

at least one processor;

at least one memory communicatively coupled to the at least one processor; and

wherein, when ~~an~~at least one encryption key needs to be used that is encrypted as an encrypted key, the at least one processor is configured to:

receive ~~at least one~~a first subset of a first set of first key components from at least a first subset of users that can be used to reconstruct the encrypted key; and

receive at least a second subset of a second set of second key components from at least a second subset of users that can be used to reconstruct the at least one encryption key used to decrypt the encrypted key into a decrypted key;

when the ~~at least one~~first subset of the first set of the first key components is received from the at least the first subset of users that can be used to reconstruct the encrypted key, reconstruct the encrypted key; and

when the at least the second subset of the at least one encryption key, reconstruct the encrypted key and second set of second key components is received from the at least the second subset of users, reconstruct the at least one encryption key; and

when the encrypted key and the at least one encryption key have both been reconstructed, decrypt the encrypted key into the decrypted key using the at least one encryption key.

16. ~~The system of claim 15, wherein the at least one processor is configured to:~~

—— receive the at least one set of key components from the at least the subset of users at least in part by being configured to receive a single set of key components;
—— reconstruct a combined string, including both the encrypted key and the at least one encryption key, from the single set of key components;
—— extracting the encrypted key and the at least one encryption key from the combined string to be used to decrypt the encrypted key into the key using the at least one encryption key.

17. — The system of claim 15, wherein the at least one processor is configured to:

—— receive the at least one set of key components from the at least the subset of users that can be used to reconstruct the encrypted key and the at least one encryption key used to decrypt the encrypted key into the key at least in part by being configured to:

—— receive a first subset of a first set of first key components from a first subset of users that can be used to reconstruct the encrypted key;

—— receive at least a second subset of at least a second set of second key components from at least a second subset of users that can be used to reconstruct at least one encryption key used to decrypt the encrypted key into the key; and

—— reconstruct the encrypted key and the at least one encryption key at least in part by being configured to:

—— when the first subset of the first set of the first key components is received from the first subset of users, reconstruct the encrypted key; and

—— when the at least the second subset of the at least the second set of the second key components is received from the at least the second subset of users, reconstruct the at least one encryption key.

18. — The system of claim 15, wherein the at least the second set of the second key components includes only a single set of key components;

—— wherein the at least the second subset of users includes only a single subset of users; and

—— wherein the at least the second set of the second key components are configured to be received from the single subset of users.

~~19~~13. The system of claim 1245, wherein the at least the second set of ~~the~~ second key components includes a plurality of sets of key components;

wherein the at least the second subset of users includes a plurality of subsets of users; and

wherein each set of key components of the plurality of sets of key components is configured to be received from a corresponding subset of users of the plurality of subsets of users.

~~20~~14. The system of claim 1245, wherein the at least one processor is configured to decrypt the encrypted key by being configured to apply at least one exclusive or (XOR) operation to the encrypted key and the at least one encryption key.

~~21~~15. The system of claim 1245, further comprising at least one network interface communicatively coupled to the at least one processor and configured to communicate with external computing devices; and

wherein when the at least one encryption key needs to be used, the at least one processor is further configured to:

cause a request for key components to be communicated to users using the at least one network interface.

~~22~~16. The system of claim 1524, wherein the request for key components is communicated to users in at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, push verify notification, polling a notification, pulling a notification, or by Bluetooth, WiFi, or near field (NFC) transmission.

~~23~~17. The system of claim 1245, wherein the first subset of users is the same subset of users as the second ~~plurality of~~ subsets of users.

~~24~~18. The system of claim 1245, wherein the at least one processor is configured to reconstruct the encrypted key and the at least one encryption key through at least one of polynomial interpolation or Shamir secret sharing.

2519. A system comprising:
at least one processor;
at least one memory communicatively coupled to the at least one processor;
at least one network interface communicatively coupled to the at least one processor and configured to communicate with external computing devices; and
wherein, when a private key needs to be used, the at least one processor is configured to:
cause a request for key components to be communicated to users using the at least one network interface;
receive ~~at least one~~ a first subset of a first set of first key components from ~~at least~~ a first subset of users that can be used to reconstruct an encrypted private key; ~~and~~
receive at least a second subset of at least as second set of second key components from at least a second subset of users that can be used to reconstruct at least one
encryption key used to decrypt the private key from the encrypted private key;
when the ~~at least one~~ first subset of the first set of ~~the~~ first key components is received from ~~the at least~~ the first subset of users that can be used to reconstruct the encrypted private key, reconstruct the encrypted private key; and
when the at least the second subset of the at least the second set of second key components is received from the at least the second subset of users ~~one encryption key,~~
reconstruct ~~the encrypted private key and~~ the at least one encryption key;
when the encrypted private key and the at least one encryption key both have been reconstructed, apply at least one exclusive or (XOR) operation to the encrypted private key and the at least one encryption key to decrypt the encrypted private key using the at least one encryption key; and
erase the private key from the at least one memory after use.

26. ~~The system of claim 25, wherein the at least one processor is configured to:~~
~~receive the at least one set of key components from the at least the subset of users at least~~
~~in part by being configured to receive a single set of key components;~~
~~reconstruct a combined string, including both the encrypted private key and the at least~~
~~one encryption key, from the single set of key components;~~

~~—extracting the encrypted private key and the at least one encryption key from the combined string to be used to decrypt the encrypted private key into the private key using the at least one encryption key.~~

27. ~~The system of claim 25, wherein the at least one processor is configured to:~~

~~—receive the at least one set of the key components from the at least the subset of users that can be used to reconstruct the encrypted private key and the at least one encryption key used to decrypt the private key from the encrypted private key at least in part by being configured to:~~

~~—receive a first subset of a first set of key components from a first subset of users that can be used to reconstruct the encrypted private key;~~

~~—receive at least a second subset of a second set of key components from at least a second subset of users that can be used to reconstruct at least one encryption key used to decrypt the encrypted private key into the key; and~~

~~—reconstruct the encrypted private key and the at least one encryption key at least in part by being configured to:~~

~~—when the first subset of the first set of the first key components is received from the first subset of users, reconstruct the encrypted private key; and~~

~~—when the at least the second subset of the second set of key components is received from the at least the second subset of users, reconstruct the at least one encryption key.~~

2820. The system of claim 1925, wherein the request for key components is communicated to users in at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, push verify notification, polling a notification, pulling a notification, or by Bluetooth, WiFi, or near field (NFC) transmission.

2921. The system of claim 1925, wherein the at least one processor is configured to reconstruct the encrypted private key and the at least one encryption key through at least one of polynomial interpolation or Shamir secret sharing.