SPLITTING ENCRYPTED KEY AND ENCRYPTION KEY USED TO ENCRYPT KEY INTO KEY COMPONENTS ALLOWING ASSEMBLY WITH SUBSET OF KEY COMPONENTS TO DECRYPT ENCRYPTED KEY

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to the following provisional patent application, each of which is hereby incorporated herein by reference:

[0002] United States Provisional Patent Application Serial No. 62/643,653 filed on March 15, 2018 and entitled "KEY SPLITTING INTO PLURALITY OF KEY COMPONENTS WITHIN SECURE ENVIRONMENT ALLOWING ASSEMBLY WITH SUBSET OF PLURALITY OF KEY COMPONENTS"; and

[0003] United States Provisional Patent Application Serial No. 62/643,655 filed on March 15, 2018 and entitled "SPLITTING ENCRYPTED KEY AND ENCRYPTION KEY USED TO ENCRYPT KEY INTO KEY COMPONENTS ALLOWING ASSEMBLY WITH SUBSET OF KEY COMPONENTS TO DECRYPT ENCRYPTED KEY".

BACKGROUND

[0004] Cryptography can be used to securely store and transmit data. Keys can be used to encrypt and decrypt data or to sign transactions.

SUMMARY

[0005] An example system includes: 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 set of key components, wherein at least a subset of key components of the at least one set of key components can be used to reconstruct the encrypted key and the at least one encryption key; and erase the key from the at least one memory.

[0006] An example system includes: 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 the 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 encryption key to generate an encrypted private key; split the encrypted private key and the at least one encryption key into at least one set of key components, wherein at least a subset of key components of the at least one set of key components can be used to reconstruct the encrypted key and the at least one encryption key; and erase the key from the at least one memory.

[0007] An example system includes: at least one processor; at least one memory communicatively coupled to the at least one processor; and wherein when an 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 set of key components from at least a subset of users that can be used to reconstruct the encrypted key and at least one encryption key used to decrypt the key from the encrypted key; when the at least the one set of key components is received from the at least the subset of users that can be used to reconstruct the encrypted key and the at least one encryption key, reconstruct the encrypted key and 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 key using the at least one encryption key.

[0008] An example system includes: 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 set of key components from at least a subset of users that can be used to reconstruct an encrypted private key and at least one encryption key used to decrypt the private key from the encrypted private key; when the at least the one set of key components is received 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, 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.

DRAWINGS

[0009] Understanding that the drawings depict only exemplary embodiments and are not therefore to be considered limiting in scope, the exemplary embodiments will be described with additional specificity and detail through the use of the accompanying drawings, in which:

[0010] Figure 1 is block diagram of an example system for securely generating, splitting, and/or reconstructing keys;

[0011] Figure 2 is a block diagrams of an example computing device used in the system of Figure 1 for securely generating, splitting and/or reconstructing keys;

[0012] Figure 3 is a block diagrams of another example computing device used in the system of Figure 1 for securely generating, splitting and/or reconstructing keys;

[0013] Figure 4 is a flow diagram of an exemplary method for securely generating and splitting a key into a plurality of key components;

[0014] Figure 5 is a flow diagram of an exemplary method for securely reconstructing a key from a subset of key components;

[0015] Figure 6 is a flow diagram of an exemplary method for securely generating at least one encryption key, using the at least one encryption key to encrypt a key into an encrypted key, and splitting the encrypted key and the at least one encryption key into a plurality of key components;

[0016] Figure 7 is a flow diagram of an exemplary method for securely reconstructing both an encrypted key and at least one encryption key from subsets of key components and securely decrypting the encrypted key using the at least one encryption key when both the encrypted key and the at least one encryption key have been reconstructed; and

[0017] Figure 8 illustrates an example of a computer system with which some embodiments of the present disclosure may be utilized.

[0018] In accordance with common practice, the various described features are not drawn to scale but are drawn to emphasize specific features relevant to the exemplary embodiments.

DETAILED DESCRIPTION

[0019] In the following detailed description, reference is made to the accompanying drawings that form a part hereof, and in which is shown by way of illustration specific illustrative embodiments. However, it is to be understood that other embodiments may be utilized and that logical, mechanical, and electrical changes may be made. Furthermore, the method presented in the drawing figures and the specification is not to be construed as limiting the order in which the individual steps may be performed. The following detailed description is, therefore, not to be taken in a limiting sense.

[0020] Keys, including cryptographic keys, can be used to encrypt and decrypt data as well as to sign transactions. Keys can include (but are not limited to) private keys, public keys, encryption keys, signing keys, and other cryptographic keys as well as passwords and secrets. In examples, a key may be embodied as a string of characters. In some configurations, one or more Advanced Encryption Standard (AES) keys may be used. An AES key may be used to symmetrically encrypt and/or decrypt data. This is referred to as "symmetric" encryption/decryption because the same key can be used to encrypt and decrypt, e.g., to encrypt and decrypt one or more private keys for different blockchain addresses, accounts, and/or wallets.

[0021] In some configurations, a keypair may be used that includes a private key and a public key. In examples, the public key can be used to encrypt data, which can only be decrypted using the private key corresponding to the public key used for encryption. In examples, a public key may be used to generate a transaction address (e.g., in a customer wallet), and only the corresponding private key can be used to sign a transaction that spends funds from the transaction address. This may be referred to as "asymmetric" encryption/decryption because the same key is not used to encrypt and decrypt (or sign transactions). It is generally desirable to keep a private key (and sometimes the public key) secure. However, there is often a tradeoff between keeping keys secure and accessible when needed.

[0022] In some instances, it is not desirable to have access to a key limited to a single person. Further, it can also be desirable that more than one person be required to use a key. In examples, this could be useful in cases where multiple directors, officers, partners, and/or

employees of an organization are required to participate when a key is used. Keys can be split into multiple parts where a subset of the parts can be used to reconstruct the keys. In examples, the generation of the components of the key can be configured to require a particular quantity of components be required to reconstruct a particular key. For example, a particular key may be split up into N key components, such that M of the N key components are required to reconstruct the particular key. In examples, the N key components can be distributed to various users. In examples, the key components can be electronically distributed to the devices of the users using at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification (such as a push verify notification), by polling (or pulling) a notification, or by Bluetooth, Wi-Fi, or near field communication (NFC) transmission. In examples, the key components can be displayed on a screen and written down or otherwise physically distributed through printing (such as into a Quick Response (QR) code, barcode, etc.) or stored on USB keys/memory sticks (or other solid state drives), or optical or magnetic disks. In examples, the key is split into the set of key components through at least one of polynomial interpolation or Shamir secret sharing.

[0023] In one configuration, an additional layer of security and flexibility can be added by using at least one encryption key (along with the key itself) to encrypt the key into an encrypted key and split apart both the encrypted key and the at least one encryption key into components such that both require a subset of key components to be reconstructed. The key components for both the encrypted key and the at least one encryption key are provided to groups of people. While the key components for the key and the encryption key could be provided to the same group of people, the groups of people could also be mutually exclusive or merely overlapping. Splitting both the encrypted key and the at least one encryption key means that collusion among the different part holders is required to maliciously reconstruct the key and encryption key. In examples, more than one of the components could be provided to the same person or entity. In examples, each component could be provided to different persons or entities.

[0024] Accordingly, the present systems and methods improve systems requiring multiple individuals/entities to hold components of keys where a number of the components are required in order to perform an action. Specifically, the present systems and methods improve such systems by securely generating and distributing the different keys/key components in a way that minimizes the possibility of malicious attacks because M of N key

components are required and, therefore, collusion between at least M part holders would be required to reconstruct the encrypted key and/or encryption key for an unauthorized purpose, while still making the encrypted key and/or encrypted key accessible when needed.

[0025] Furthermore, some configurations of the present systems and methods are more secure than conventional key splitting because the components of the encrypted key are encrypted before distribution to part holders. Therefore, even if the key components for the encrypted key are intercepted, the encrypted key could only be reconstructed if the encryption key is also reconstructed based on the encryption key components. In other words, the additional layer of encryption with the encryption key and splitting reduces the possibility of a malicious actor reconstructing the asset encryption key without getting enough components parts from both the encrypted key and the encryption key.

[0026] Figure 1 is block diagram of an example system 100 for securely generating, splitting, and/or reconstructing keys. System 100 includes a computing device 102 and a plurality of optional computing devices 104 (such as optional computing devices 104-1 through optional computing devices 104-A). Each of computing device 102 and computing devices 104 can be implemented as any of a mobile computing device, such as a mobile phone, tablet computer, mobile media device, mobile gaming device, laptop computer, vehicle-based computer, etc.; or a non-mobile device such as a dedicated terminal, a public terminal, a kiosk, a server, or a desktop computer. Each computing device 104 is communicatively coupled to the computing device 102 using at least one network 106 (such as network 106-1 through network 106-A). In examples, the at least one network 106 includes at least one wired network and/or at least one wireless network. In examples, any combination of wired and wireless networks is used to couple the computing devices 104 to the computing device 102. In examples, the at least one network 106 includes at least one of at least one local area network (LAN), at least one wide area network (WAN), or the Internet. In examples, any combination of local area networks, wide area networks, or the Internet is used as the at least one network 106 to couple the computing devices 104 to the computing device 102. In examples, each of computing device 102 and computing devices 104 includes at least one memory, at least one processor, at least one optional network interface, at least one optional display device, at least one optional input device, and at least one power source.

[0027] Figures 2 and 3 are block diagrams of example computing devices. Figure 2 is a block diagram of an example computing device 102 used in system 100 for securely generating, splitting and/or reconstructing keys. Computing device 102 includes at least one

memory 202, at least one processor 204, optional at least one network interface 206, optional key generating module 208, optional key splitting module 210, optional key reconstructing module 212, optional display device 214, optional input device 216, and optional power source 218. Figure 3 is a block diagram of an example computing device 104 used in system 100 for securely generating, splitting and/or reconstructing keys. Computing device 104 includes at least one memory 302, at least one processor 304, optional at least one network interface 306, optional component receipt module 308, optional authorization module 310, optional component communication module 312, optional display device 314, optional input device 316, and optional power source 318.

[0028] In examples, the at least one memory 202 and/or the at least one memory 302 can be any device, mechanism, or populated data structure used for storing information. In examples, the at least one memory 202 and/or the at least one memory 302 can be or include any type of volatile memory, nonvolatile memory, and/or dynamic memory. For example, the at least one memory 202 and/or the at least one memory 302 can be random access memory, memory storage devices, optical memory devices, magnetic media, floppy disks, magnetic tapes, hard drives, erasable programmable read-only memories (EPROMs), electrically erasable programmable read-only memories (EEPROMs), optical media (such as compact discs, DVDs, Blu-ray Discs) and/or the like. In accordance with some embodiments, the at least one memory 202 and/or the at least one memory 302 may include one or more disk drives, flash drives, one or more databases, one or more tables, one or more files, local cache memories, processor cache memories, relational databases, flat databases, and/or the like. In addition, those of ordinary skill in the art will appreciate many additional devices and techniques for storing information which can be used as the at least one memory 202 and/or the at least one memory 302. The at least one memory 202 and/or the at least one memory 302 may be used to store instructions for running one or more applications or modules on the at least one processor 204 and/or the at least one processor 304. For example, the at least one memory 202 could be used in one or more examples to house all or some of the instructions needed to execute the functionality of the optional key generating module 208, optional key splitting module 210, and optional key reconstructing module 212. Similarly, the at least one memory 302 could be used in one or more examples to house all or some of the instructions needed to execute the functionality of the optional component receipt module 308, the optional authorization module 310, and the optional component communication module 312.

[0029] The at least one processor 204 and/or the at least one processor 304 can be any known processor, such as a general purpose processor (GPP) or special purpose (such as a field-programmable gate array (FPGA), application-specific integrated circuit (ASIC) or other integrated circuit or circuitry), or any programmable logic device. In examples, any of the at least one key generating module 208, key splitting module 210, and/or key reconstructing module 212 are implemented by the at least one processor 204 and the at least one memory 202. In examples, any of the at least one component receipt module 308, authorization module 310, and/or component communication module 312 are implemented by the at least one processor 304 and the at least one memory 302.

[0030] In examples, the at least one optional network interface 206 and/or the at least one optional network interface 206 includes or is coupled to at least one optional antenna for communication with a network (such as one of the at least one networks 106 of system 100). In examples, the at least one optional network interface 306 includes or is coupled to at least one optional antenna for communication with a network (such as one of the at least one networks 106 of system 100). In examples, the at least one optional network interface 206 and/or the at least one optional network interface 206 includes at least one of an Ethernet interface, a cellular radio access technology (RAT) radio, a Wi-Fi radio, a Bluetooth radio, or a near field communication (NFC) radio. In examples, the at least one optional network interface 206 and/or the at least one optional network interface 206 includes a cellular radio access technology radio configured to establish a cellular data connection (mobile internet) of sufficient speeds with a remote server using a local area network (LAN) or a wide area network (WAN). In examples, the cellular radio access technology includes at least one of Personal Communication Services (PCS), Specialized Mobile Radio (SMR) services, Enhanced Special Mobile Radio (ESMR) services, Advanced Wireless Services (AWS), Code Division Multiple Access (CDMA), Global System for Mobile Communications (GSM) services, Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Worldwide Interoperability for Microwave Access (WiMAX), 3rd Generation Partnership Projects (3GPP) Long Term Evolution (LTE), High Speed Packet Access (HSPA), third generation (3G) fourth generation (4G), fifth generation (5G), etc. or other appropriate communication services or a combination thereof. In examples, the at least one optional network interface 206 and/or the at least one optional network interface 206 includes a Wi-Fi (IEEE 802.11) radio configured to communicate with a wireless local area network that communicates with the remote server, rather than a wide

area network. In examples, the at least one optional network interface 206 and/or the at least one optional network interface 206 includes a near field radio communication device that is limited to close proximity communication, such as a passive near field communication (NFC) tag, an active near field communication (NFC) tag, a passive radio frequency identification (RFID) tag, an active radio frequency identification (RFID) tag, a proximity card, or other personal area network device. In examples, the same at least one optional network interface 206 and/or the at least one optional network interface 206 is also used for communication with an external gateway device to a network (such as an NFC payment terminal).

[0031] In examples, the optional at least one display device 214 and/or the optional at least one display device 314 includes at least one of a light emitting diode (LED), a liquid crystal display (LCD), a light emitting diode (LED) display, an organic light emitting diode (OLED) display, an e-ink display, a field emission display (FED), a surface-conduction electron-emitter display (SED), or a plasma display. In examples, the optional at least one input device 216 include at least one of a touchscreen (including capacitive and resistive touchscreens), a touchpad, a capacitive button, a mechanical button, a switch, a dial, a keyboard, a mouse, a camera, a biometric sensor/scanner, etc. In examples, the optional at least one display device 214 and/or the optional at least one display device 314 and the optional at least one input device 216 are combined into a human machine interface (HMI) for user interaction with the computing device 102.

[0032] In examples, at least one optional power source 218 is used to provide power to the various components of the network node 102. In examples, at least one optional power source 318 is used to provide power to the various components of the network node 104.

[0033] The at least one processor 204 of the computing device 102 is configured to securely generate at least one key. In examples, this is implemented in the key generating module 208. The at least one processor 204 of the computing device 102 may be configured to securely generate the at least one key randomly. In examples, the at least one processor 204 of the computing device 102 may implement a key generator to securely generate the at least one key. In examples, the key generator includes at least one of linear feedback shift register (LFSR), Solitaire cipher, and/or Pontifex cipher. In examples, the at least one processor 204 of the computing device 102 is configured to generate the at least one key by generating a sequence having many pseudo-random characteristics. In examples, the key can be used to encrypt and/or decrypt data. To enable secure generation of the at least one key, the at least one processor 204 may be configured to generate at least one key by first verifying that no

users are logged into the computing device 102. To enable secure generation of the at least one key, the at least one processor 204 may be configured to check that the computing device 102 is not being implemented as a virtual machine. To enable secure generation of the at least one key, the at least one processor 204 may be configured to block user logins into the system.

[0034] The at least one processor 204 is further configured to split the key into a set of key components where at least one subset of the key components can be used to reconstruct the key. In examples, this is implemented in the key splitting module 210. In examples, the split of the key into the set of key components is configurable, such that a particular quantity of key components may be required to reconstruct the key. For example, a particular key may be split up into N key components, such that M of the N key components are required to reconstruct the particular key. In examples, the key components are distributed to various users. In examples, the key components can be electronically distributed to user devices using the at least one network interface 206, such as by at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, or push verify notification. In examples, the key is split into the set of key components through at least one of polynomial interpolation or Shamir secret sharing. In examples, the key components can be displayed, printed, or otherwise fixed on a medium provided to users that could then input the key component into their corresponding computing device 104.

[0035] In examples, an additional layer of security and flexibility can be added by using at least one encryption key along with the key to encrypt the key itself into an encrypted key and split apart both the encrypted key itself and the at least one encryption key such that both require a subset of key components to be reconstructed. In examples, the at least one processor 204 is configured to encrypt the key by applying at least one exclusive or (XOR) operation to the key and the at least one encryption key. In examples, the encrypted key is configured to include a one in each bit position where bits in a corresponding bit position in both the key and the at least one encryption key are different; and the encrypted key is configured to include a zero in each bit position where bits in the corresponding bit position in both the key and the at least one encryption key are the same. In examples where the at least one encryption key includes a plurality of encryption keys, the a least one processor 204 is configured to apply a first exclusive or (XOR) between the key and the first of the plurality of encryption keys, then a second exclusive or (XOR) between the result of the first XOR and a second of the plurality of encryption keys, and so forth until all of the plurality of

encryption keys have been used. In examples, only one encryption key is used by the at least one processor 204 to encrypt the key itself before the key itself and the encryption key are split and provided to various users. In examples, a plurality of encryption keys are used by the at least one processor 204 to encrypt the key itself before the key itself and the plurality of encryption keys are split and provided to various users. In examples, they key components for both the encrypted key itself and the at least one encryption key are provided to groups of people. While the key components for the at least one encryption key and the encrypted key could be provided to the same group of people, the two groups of people could also be mutually exclusive or merely overlapping.

[0036] In examples, the at least one processor 204 is configured to combine the encrypted key and the at least one encryption key together before splitting the encrypted key and the at least one encryption key into the at least one set of key components that can be provided to a plurality of users. For example, the at least one processor 204 can be configured to concatenate the encrypted key and the at least one encryption key together into a string and then split the string into the at least one set of key components that can be provided to a plurality of users. In examples, the at least one processor 204 can be configured to split apart the encrypted key and the at least one set of key components into separate sets of key components that can be provided to a plurality of users. For example, the at least one processor 204 can be configured to split the encrypted key into a first set of key components that can be provided to a first plurality of users, wherein at least a first subset of the first key components can be used to reconstruct the encrypted key. Similarly, the at least one processor 204 can be configured to split each encryption key of the at least one encryption key into at least second key components that can be provided to at least a second plurality of users, wherein at least a second subset of the at least the second key components can be used to reconstruct the at least one encryption key.

[0037] In examples, the at least one processor 304 for a computing device 104 for a user is configured to receive key components generated by the computing device 102 and configured to store the key component in the at least one memory 302. In exemplary embodiments, this is implemented in the component receipt module 308. In examples, the at least one processor 304 of the computing device 104 is configured to securely receive at least one key component via the at least one network interface 306 (such as being received electronically from the computing device 102). In examples, the key components can be electronically received at the computing device 104 using the at least one network interface 306, such as by at least one

of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, or push verify notification. In examples, the at least one processor 304 of the computing device is configured to receive at least one key component via the at least one input device 316 (such as being manually entered into the system 106 by a user). In examples, the key components can be input manually input into the computing device 104 using the input device 316, such as by a touchscreen, keyboard, mouse, or a media reader. To enable secure receipt of the at least one key component, the at least one processor 304 may be configured to: receive the at least one key component only after verifying that no users are logged into the computing device 104; check that the computing device 104 is not being implemented as a virtual machine; and block other user logins into the computing device 104.

[0038] In examples, the at least one processor 204 of the computing device 102 is further configured to reconstruct the key from a set of key components where at least one subset of the key components can be used to reconstruct the key. In examples, this is implemented in the key reconstructing module 212. In examples, the at least one processor 204 is configured to transmit a request to a plurality of computing devices 104 for a plurality of users to provide key components so that the key can be reconstructed. In examples, the request can be electronically transmitted from the computing device 102 using the at least one network interface 206, such as by at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, or push verify notification.

[0039] In examples, the at least one processor 204 is configured to receive at least one subset of the key components from a plurality of users, where the subset of the set of key components can be used to reconstruct the key. In examples, the at least one processor 204 is configured to securely reconstruct the key when the subset of the set of key components is received from the plurality of users. In examples, at least some of the subset of key components is received from the plurality of users via the at least one network interface 206 (such as being received electronically from user devices, such as a computing device 104). In examples, at least some of the subset of key components is received from the plurality of users via the at least one input device 216 (such as being manually entered into the system 104 by users).

[0040] In examples, the at least one processor 304 of a computing device 104 for a user is configured to receive a request from the computing device 102 for users to provide key components so that the key can be reconstructed. In examples, the request can be

electronically received at the computing device 104 using the at least one network interface 306, such as by at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, or push verify notification. In examples, the at least one processor 304 is configured to cause the display device 314 to display the request for users to provide key components so that the key can be reconstructed. In examples, the at least one processor 304 is configured to receive user input via the display device 314. In examples, the user input is a response confirming or declining the request (such as using a push verify notification) where they system can access the key component from the at least one memory 302 and communicate it to the computing device 102 in response to the user confirming the request or provide a message back to the computing device 102 in response to the user declining the request. In examples, the user input is the actual key component itself (such as manual entry of the key component using the input device 316) which can then be communicated to the computing device 102.

[0041] In examples, an additional layer of security is provided by keys split to various users which can help with the situation where some or all of the key subsets become lost, comprised, etc. without having the change the key itself. In examples, it may make sense to generate a new set of key components to be provided to individuals when key subsets are lost, compromised, etc. or when the group of individuals who have the key subsets should be changed (such as when an executive, other employee, or director departs or changes their position). In such cases, a sufficient quantity of key components are received back at the at least one processor 204 and the at least one processor 204 is configured to regenerate the key itself or the encrypted key and any encryption keys necessary to decrypt the encrypted key into the key itself where the at least one processor 204 is configured to decrypt the encrypted key using any required encryption keys to obtain the key. One or more new encryption keys can be generated and used to encrypt the key. The key and the one or more new encryption keys can be split apart as described above into components and the components provided to one or more groups of people as desirable.

[0042] In examples, the at least one set of key components includes a single set of key components and the at least one processor 204 is configured to reconstruct the encrypted key and the at least one encryption key at least in part by being configured to: reconstruct a combined string, including both the encrypted key and the at least one encryption key, from the single set of key components; and extract the encrypted key and the at least one encryption key from the combined string to be used to securely decrypt the encrypted key

into the key using the at least one encryption key. In examples, the at least one processor 204 is configured to receive the at least one subset of key components from the at least one subset of users that can be used to reconstruct the encrypted key and the at least one encryption 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 key; and receive at least a second subset of key components of at least 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 securely decrypt the key from the encrypted key. In some of these examples, the at least one processor 204 is configured to 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 key components is received from the first subset of users, securely reconstruct the encrypted key; and when the at least the second subset of key components of the at least the second key components is received from the at least the second subset of users, securely reconstruct the at least one encryption key. In examples, the at least one processor 204 is configured to decrypt the encrypted key using the at least one encryption key at least in part by applying at least one exclusive or (XOR) operation to the encrypted private key and the at least one encryption key to securely. In examples, the at least one processor is configured to securely erase the private key from the at least one memory after use.

[0043] Figure 4 is a flow diagram of an example method 400 for securely generating and splitting a key (such as a private key used in asymmetrical cryptography). Example method 400 begins at optional block 402 with optionally blocking user logins into the system. In examples, blocking user logins into the system occurs at least in part by blocking secure shell (SSH) logins and/or any other access into the system. Example method 400 proceeds to optional block 404 with optionally verifying that no users are logged into a system. Example method 400 proceeds to optional block 406 with optionally checking that the system is not implemented as a virtual machine. Example method 400 proceeds to block 408 with securely generating a key (such as a private key used in asymmetrical cryptography). Example method 400 proceeds to block 410 with splitting the key into a set of key components where at least one subset of the key components can be used to reconstruct the key. Example method 400 proceeds to block 412 with securely erasing the key from memory. In examples, securely erasing the key from the key from memory using a DoD memory wipe. Example method 400 proceeds to optional block 414 with optionally communicating the set of key components to remote devices 414. In examples, the set of key components are

communicated to users in at least one of email, Short Message Service (SMS), Multimedia Messaging Service (MMS), instant messaging, push notification, or push verify notification.

[0044] Figure 5 is a flow diagram of an example method 500 for securely reconstructing a key (such as a private key used in asymmetrical cryptography) from a subset of key components. Example method 500 begins at optional block 502 with optionally communicating a request for key components to user devices. Example method 500 proceeds to optional block 504 with optionally blocking user logins into a system. Example method 500 proceeds to optional block 506 with optionally verifying that no users are logged into the system. Example method 500 proceeds to optional block 508 with optionally checking that the system is not implemented as a virtual machine. Example method 500 proceeds to block 510 with receiving a subset of a set of key components from a plurality of users where the subset of the set of key components can be used to reconstruct the key. Example method 500 proceeds to block 512 with securely reconstructing the key when the subset of key components is received from the plurality of users. Example method 500 proceeds to optional block 514 with optionally securely erasing the key from memory after use.

[0045] Figure 6 is a flow diagram of an example method 600 for securely generating at least one encryption key, using the at least one encryption key to encrypt a key (such as a private key, a public key, an encryption key, a signing key, or another cryptographic key or a password or secret) into an encrypted key, and splitting the encrypted key and the at least one encryption key into a plurality of key components. Example method 600 begins at optional block 602 with optionally blocking user logins into a system. Example method 600 proceeds to optional block 604 with optionally verifying that no users are logged into a system. Example method 600 proceeds to optional block 606 with optionally checking that the system is not implemented as a virtual machine. Example method 600 proceeds to optional block 608 with optionally securely generating a key (such as a private key, a public key, an encryption key, a signing key, or another cryptographic key or a password or secret).

[0046] Example method 600 proceeds to block 610 with securely generating at least one encryption key. Example method 600 proceeds to block 612 with encrypting the key using the at least one encryption key to generate an encrypted key. In examples, the key is encrypted by applying at least one exclusive or (XOR) operation to the key and the at least one encryption key. In examples, the encrypted key is configured to include a one in each bit position where bits in a corresponding bit position in both the key and the at least one encryption key are different; and the encrypted key is configured to include a zero in each bit

position where bits in the corresponding bit position in both the key and the at least one encryption key are the same. In examples where the at least one encryption key includes a plurality of encryption keys, a first exclusive or (XOR) can be applied between the key and the first of the plurality of encryption keys, then a second exclusive or (XOR) between the result of the first XOR and a second of the plurality of encryption keys, and so forth until all of the plurality of encryption keys have been used.

[0047] Example method 600 proceeds to block 614 with splitting the encrypted key and the at least one encryption key into at least one set of key components, wherein at least a subset of key components of the at least one set of key components can be used to reconstruct the encrypted key and the at least one encryption key. In examples, the encrypted key and the at least one encryption key are combined together before splitting the encrypted key and the at least one encryption key into the at least one set of key components that can be provided to a plurality of users. For example, the encrypted key and the at least one encryption key can be concatenated together into a string that is then split into at the at least one set of key components that can be provided to a plurality of users. In examples, the encrypted key and the at least one set of key components can be split apart into separate sets of key components that can be provided to a plurality of users. For example, the encrypted key can be split into a first set of key components that can be provided to a first plurality of users, wherein at least a first subset of the first key components can be used to reconstruct the encrypted key. Similarly, each encrypted key of the at least one encryption key can be split into at least second key components that can be provided to at least a second plurality of users, wherein at least a second subset of the at least second key components can be used to reconstruct the at least one encryption key.

[0048] Example method 600 proceeds to block 616 with securely erasing the key, the at least one encryption key, and/or the encrypted key from memory. In examples, example method 600 proceeds to optional block 618 with optionally communicating sets of key components to remote devices. In examples, the sets of key components are securely 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, Wi-Fi, or near field (NFC) transmission.

[0049] Figure 7 is a flow diagram of an example method 700 for securely reconstructing bon an encrypted key and at least one encryption key from subsets of key components and securely decrypting the encrypted key using the at least one encryption key when both the

encrypted key and the at least one encryption key have been reconstructed. Example method 700 begins at block 702 with optionally communicating a request for key components to user devices. In exemplary embodiments, the request for key components is securely 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, Wi-Fi, or near field (NFC) transmission.

[0050] Example method 700 proceeds to optional block 704 with optionally blocking user logins into the system. Example method 700 proceeds to optional block 706 with optionally verifying that no users are logged into a system. Example method 700 proceeds to optional block 708 with optionally checking that the system is not implemented as a virtual machine. Example method 700 proceeds to optional block 710 with receiving at least one subset of key components from at least one subset of users that can be used to reconstruct the encrypted key and the at least one encryption key. Example method 700 proceeds to block 712 with reconstructing the encrypted key and the at least one encryption key when at least one set of key components is received from at least one subset of users that can be used to reconstruct the encrypted key and the at least one encryption key. In examples, the at least one set of key components includes a single set of key components and reconstructing the encrypted key and the at least one encryption key includes: reconstructing a combined string, including both the encrypted key and the at least one encryption key, from the single set of key components; and extracting the encrypted key and the at least one encryption key from the combined string to be used to securely decrypt the encrypted key into the key using the at least one encryption key.

[0051] In examples, receiving the at least one subset of key components from the at least one subset of users that can be used to reconstruct the encrypted key and the at least one encryption key includes: receiving a first subset of a first set of key components from a first subset of users that can be used to reconstruct the encrypted key; and receiving at least a second subset of key components of at least 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 securely decrypt the key from the encrypted key. In some of these examples, securely reconstructing the encrypted key and the at least one encryption key includes: when the first subset of the first key components is received from the first subset of users, securely reconstructing the encrypted key; and when the at least the second subset of key components

of the at least the second key components is received from the at least the second subset of users, securely reconstructing the at least one encryption key. Example method 700 proceeds to block 716 with optionally securely erasing the key, the encrypted key, and/or the at least one encryption key after use.

[0052] The techniques introduced here can be embodied as special-purpose hardware (such as circuitry), as programmable circuitry appropriately programmed with software and/or firmware, or as a combination of special-purpose and programmable circuitry. Hence, embodiments may include a machine-readable medium having stored thereon instructions that may be used to program a computer (or other electronic devices) to perform a process. The machine-readable medium may include, for example, floppy diskettes, optical disks, compact disc read-only memories (CD-ROMs), magneto-optical disks, read-only memories (ROMs), random access memories (RAMs), erasable programmable read-only memories (EPROMs), electrically erasable programmable read-only memories (EEPROMs), magnetic or optical cards, flash memory, or other type of media/machine-readable medium suitable for storing electronic instructions.

[0053] **Computer System Overview**

[0054] Embodiments of the present disclosure include various steps and operations, which have been described above. A variety of these steps and operations may be performed by hardware components or may be embodied in machine-executable instructions, which may be used to cause a general-purpose or special-purpose processor programmed with the instructions to perform the steps. Alternatively, the steps may be performed by a combination of hardware, software, and/or firmware. As such, Figure 8 is an example of a computer system 800 with which embodiments of the present disclosure may be utilized. According to the present example, the computer system 800 includes an interconnect 802, at least one processor 804, at least one communication port 806, at least one main memory 808, at least one removable storage media 810, at least one read only memory 812, and at least one mass storage device 814.

[0055] The at least one processor 804 can be any known processor. The at least one communication port 806 can be or include, for example, any of an RS-232 port for use with a modem-based dialup connection, a 10/100 Ethernet port, or a Gigabit port using copper or fiber. The nature of the at least one communication port 806 may be chosen depending on a network such a Local Area Network (LAN), Wide Area Network (WAN), or any network to

which the computer system 800 connects. The at least one main memory 808 can be Random Access Memory (RAM), or any other dynamic storage device(s) commonly known in the art. The at least one read only memory 812 can be any static storage device(s) such as Programmable Read Only Memory (PROM) chips for storing static information such as instructions for the at least one processor 804.

[0056] The at least one mass storage device 814 can be used to store information and instructions. For example, hard disks (such as magnetic disk drives or solid state drive using serial/parallel ATA or SCSI interfaces), an optical disc, an array of disks such as a Redundant Array of Independent Disks (RAID), or any other mass storage devices may be used. Interconnect 802 can be or include one or more buses, bridges, controllers, adapters, and/or point-to-point connections. Interconnect 802 communicatively couples the at least one processor 804 with the other memory, storage, and communication blocks. Interconnect 802 can be a PCI/PCI-X or SCSI based system bus depending on the storage devices used. The at least one removable storage media 810 can be any kind of external hard-drives, floppy drives, Compact Disc–Read Only Memory (CD-ROM), Compact Disc–Re-Writable (CD-RW), Digital Video Disc–Read Only Memory (DVD-ROM), Blu-Ray Disc Read Only Memory (BD-ROM), Blu-Ray Disc Recordable (BD-R), Blu-Ray Disc Recordable Erasable (BD-RE).

[0057] The components described above are meant to exemplify some types of possibilities. In no way should the aforementioned examples limit the disclosure, as they are only exemplary embodiments. The embodiments, structure, methods, etc. described herein, including those below and above, can be combined together in various ways.

[0058] **<u>Terminology</u>**

[0059] Brief definitions of terms, abbreviations, and phrases used throughout this application are given below.

[0060] The terms “connected”, “coupled”, and “communicatively coupled” and related terms are used in an operational sense and are not necessarily limited to a direct physical connection or coupling. Thus, for example, two devices may be coupled directly, or via one or more intermediary media or devices. As another example, devices may be coupled in such a way that information can be passed there between, while not sharing any physical connection with one another. Based on the disclosure provided herein, one of ordinary skill in the art will appreciate a variety of ways in which connection or coupling exists in accordance with the aforementioned definition.

[0061] The phrase “based on” does not mean “based only on,” unless expressly specified otherwise. In other words, the phrase “based on” describes both “based only on” and “based at least on”. Additionally, the term “and/or” means “and” or “or”. For example, “A and/or B” can mean “A”, “B”, or “A and B”. Additionally, “A, B, and/or C” can mean “A alone,” “B alone,” “C alone,” “A and B,” “A and C,” “B and C” or “A, B, and C.”

[0062] The phrases “in exemplary embodiments”, “in example embodiments”, “in some embodiments”, “according to some embodiments”, “in the embodiments shown”, “in other embodiments”, “embodiments”, “in examples”, “examples”, “in some examples”, “some examples” and the like generally mean the particular feature, structure, or characteristic following the phrase is included in at least one embodiment of the present disclosure, and may be included in more than one embodiment of the present disclosure. In addition, such phrases do not necessarily refer to the same embodiments or different embodiments.

[0063] If the specification states a component or feature “may,” “can,” “could,” or “might” be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

[0064] The term “responsive” includes completely or partially responsive.

[0065] The term “module” refers broadly to a software, hardware, or firmware (or any combination thereof) component. Modules are typically functional components that can generate useful data or other output using specified input(s). A module may or may not be self-contained. An application program (also called an “application”) may include one or more modules, or a module can include one or more application programs.

[0066] The term “network” generally refers to a group of interconnected devices capable of exchanging information. A network may be as few as several personal computers on a Local Area Network (LAN) or as large as the Internet, a worldwide network of computers. As used herein, “network” is intended to encompass any network capable of transmitting information from one entity to another. In some cases, a network may be comprised of multiple networks, even multiple heterogeneous networks, such as one or more border networks, voice networks, broadband networks, financial networks, service provider networks, Internet Service Provider (ISP) networks, and/or Public Switched Telephone Networks (PSTNs), interconnected via gateways operable to facilitate communications between and among the various networks.

[0067] Also, for the sake of illustration, various embodiments of the present disclosure have herein been described in the context of computer programs, physical components, and logical interactions within modern computer networks. Importantly, while these embodiments describe various embodiments of the present disclosure in relation to modern computer networks and programs, the method and apparatus described herein are equally applicable to other systems, devices, and networks as one skilled in the art will appreciate. As such, the illustrated applications of the embodiments of the present disclosure are not meant to be limiting, but instead are examples. Other systems, devices, and networks to which embodiments of the present disclosure are applicable include, for example, other types of communication and computer devices and systems. More specifically, embodiments are applicable to communication systems, services, and devices such as cell phone networks and compatible devices. In addition, embodiments are applicable to all levels of computing from the personal computer to large network mainframes and servers.

[0068] In conclusion, the present disclosure provides novel systems, methods, and arrangements for securely splitting, distributing, and/or reconstructing keys. While detailed descriptions of one or more embodiments of the disclosure have been given above, various alternatives, modifications, and equivalents will be apparent to those skilled in the art without varying from the spirit of the disclosure. For example, while the embodiments described above refer to particular features, the scope of this disclosure also includes embodiments having different combinations of features and embodiments that do not include all of the described features. Accordingly, the scope of the present disclosure is intended to embrace all such alternatives, modifications, and variations as fall within the scope of the claims, together with all equivalents thereof. Therefore, the above description should not be taken as limiting.

Example Embodiments

[0069] Example 1 includes 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 set of key components, wherein at least a subset of key components of the at least one set of key components can be used to reconstruct the encrypted key and the at least one encryption key; and erase the key from the at least one memory.

[0070] Example 2 includes the system of Example 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 and the at least one encryption key into the at least one set of key components.

[0071] Example 3 includes the system of any of Examples 1-2, wherein the at least one processor is configured to split the encrypted key and the at least one encryption key into 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 key components can be used to reconstruct the encrypted key, wherein the first set of 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 at least second key components, wherein at least a second subset of the at least second key components can be used to reconstruct the at least one encryption key, wherein the at least the second set of key components are configured to be provided to at least a second plurality of users.

[0072] Example 4 includes the system of Example 3, wherein the at least the second set of the at least second key components includes only a single set of key components; wherein the at least the second plurality of users includes only a single set of users; and wherein the at least the second set of key components are configured to be provided to the single set of users.

[0073] Example 5 includes the system of any of Examples 3-4, wherein the at least the second set of the at least second key components includes a plurality of sets of key components; wherein the at least 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.

[0074] Example 6 includes the system of any of Examples 1-5, 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.

[0075] Example 7 includes the system of any of Examples 1-6, 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.

[0076] Example 8 includes the system of any of Examples 1-7, wherein the encrypted key is configured to include a one in each bit position where bits in a corresponding bit position in both the key and the at least one encryption key are different; wherein the encrypted key is

configured to include a zero in each bit position where bits in the corresponding bit position in both the key and the at least one encryption key are the same.

[0077] Example 9 includes the system of any of Examples 1-8, wherein prior to generating the key when the key needs to be generated, the at least one processor is configured to: block user logins into the system; verify that no users are logged into the system; and check that the system is not being implemented as a virtual machine.

[0078] Example 10 includes the system of Example 9, wherein the at least one processor is configured to block user logins into the system at least in part by being configured to: block secure shell (SSH) logins into the system.

[0079] Example 11 includes the system of any of Examples 1-10, wherein the at least one processor is configured to erase the key from the at least one memory using a DoD memory wipe.

[0080] Example 12 includes the system of any of Examples 1-11, 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: receive the third subset of the first set of key components from the first subset of users using encrypted communication; and receive the fourth subset of the at least the second set of key components from the second subset of users using encrypted communication.

[0081] Example 13 includes the system of any of Examples 1-12, further comprising: at least one network interface communicatively coupled to the at least one processor and configured to communicate with external computing devices.

[0082] Example 14 includes the system of Example 13, wherein when the key needs to be generated, the at least one processor is further configured to: cause the at least one network interface to communicate the first set of key components to 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 key components to computing devices for the second plurality of users.

[0083] Example 15 includes the system of Example 14, wherein at least one of the first set of key components and the at least the second set of 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, Wi-Fi, or near field (NFC) transmission.

[0084] Example 16 includes the system of any of Examples 13-15, wherein when the key needs to be used, the at least one processor is configured to: when a third subset of the first

set of key components is received from a first subset of users that can be used to reconstruct the encrypted key, reconstruct the encrypted key; when a fourth subset of the at least the second set of key components is received from a second subset of users that can be used to reconstruct the at least one encryption key, reconstruct the at least one encryption key; when the encrypted key and the at least one encryption key have both been reconstructed, decrypt the encrypted key into the key using the at least one encryption key.

[0085] Example 17 includes the system of Example 16, wherein the first plurality of users are the same plurality of users as the second plurality of users.

[0086] Example 18 includes the system of any of Examples 13-17, wherein when the 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; when a third subset of the first set of key components is received from a first subset of users that can be used to reconstruct the encrypted key, reconstruct the encrypted key; when a fourth subset of the at least the second set of key components is received from a second subset of users that can be used to reconstruct the at least one encryption key, reconstruct the at least one encryption key; when the encrypted key and the at least one encryption key have both been reconstructed, decrypt the encrypted key using the at least one encryption key.

[0087] Example 19 includes the system of Example 18, wherein the request for key components is communicated to users using encrypted communication; wherein the third subset of the first set of key components is received from the first subset of users using encrypted communication; and wherein the fourth subset of the at least the second set of key components is received from the second subset of users using encrypted communication.

[0088] Example 20 includes the system of any of Examples 18-19, 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, Wi-Fi, or near field (NFC) transmission.

[0089] Example 21 includes the system of any of Examples 18-20, wherein the first plurality of users are the same plurality of users as the second plurality of users; and wherein the first subset of users is the same subset of users as the second subset of users.

[0090] Example 22 includes the system of any of Examples 1-21, wherein the at least one processor is configured to split the encrypted key and the at least one encryption key into at least one set of key components through at least one of polynomial interpolation or Shamir secret sharing.

[0091] Example 23 includes the system of any of Examples 1-22, wherein at least one of the at least one encryption key and the key is a private key used in asymmetrical cryptography.

[0092] Example 24 includes 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 the 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 encryption key to generate an encrypted private key; split the encrypted private key and the at least one encryption key into at least one set of key components, wherein at least a subset of key components of the at least one set of key components can be used to reconstruct the encrypted key and the at least one encryption key; and erase the key from the at least one memory.

[0093] Example 25 includes the system of Example 24, 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 and the at least one encryption key into the at least one set of key components.

[0094] Example 26 includes the system of any of Examples 1-25, wherein the at least one processor is configured to split the encrypted key and the at least one encryption key into 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 key components can be used to reconstruct the encrypted private key, wherein the first set of 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 at least second key components, wherein at least a second subset of the at least the second key components can be used to reconstruct the at least one encryption key, wherein the at least the second set of key components are configured to be provided to at least a second plurality of users.

[0095] Example 27 includes the system of any of Examples 24-26, wherein the at least one processor is further configured to: cause the at least one network interface to communicate the first set of key components to 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 key components to computing devices for the second plurality of users.

[0096] Example 28 includes the system of Example 27, wherein at least one of the first set of key components and the at least the second set of 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, Wi-Fi, or near field (NFC) transmission.

[0097] Example 29 includes the system of any of Examples 24-28, wherein when the private key needs to be used, the at least one processor is configured to: when a third subset of the first set of key components is received from a first subset of users that can be used to reconstruct the encrypted private key, reconstruct the encrypted private key; when a fourth subset of the at least the second set of key components is received from a second subset of users that can be used to reconstruct the at least one encryption key, reconstruct the at least one encryption key; and when the encrypted private key and the encryption key have both 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.

[0098] Example 30 includes the system of any of Examples 24-29, wherein when the 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; when a third subset of the first set of key components is received from a first subset of users that can be used to reconstruct the encrypted private key, reconstruct the encrypted private key; when a fourth subset of the at least the second set of key components is received from a second subset of users that can be used to reconstruct the at least one encryption key, reconstruct the at least one encryption key; when the encrypted private key and the at least one encryption key have both been reconstructed, decrypt the encrypted private key using the at least one encryption key.

[0099] Example 31 includes the system of Example 30, 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, Wi-Fi, or near field (NFC) transmission.

[0100] Example 32 includes the system of any of Examples 24-31, wherein the at least one processor is configured to split the encrypted private key and the at least one encryption key into at least one set of key components through at least one of polynomial interpolation or Shamir secret sharing.

[0101] Example 33 includes a system comprising: at least one processor; at least one memory communicatively coupled to the at least one processor; and wherein when an 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 set of key components from at least a subset of users that can be used to reconstruct the encrypted key and at least one encryption key used to decrypt the key from the encrypted key; when the at least the one set of key components is received from the at least the subset of users that can be used to reconstruct the encrypted key and the at least one encryption key, reconstruct the encrypted key and 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 key using the at least one encryption key.

[0102] Example 34 includes the system of Example 33, 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.

[0103] Example 35 includes the system of any of Examples 33-34, wherein the at least one processor is configured to: receive at least one set of key components from at least a subset of users that can be used to reconstruct the encrypted key and at least one encryption key used to decrypt the key from the encrypted 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 key; receive at least a second subset of key components of at least 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 key from the encrypted 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 key components is received from the first subset of users, reconstruct the encrypted key; and when the at least the second subset of key components of the at least the second key components is received from the at least the second subset of users, reconstruct the at least one encryption key.

[0104] Example 36 includes the system of any of Examples 33-35, wherein the at least the second set of key components of the at least 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 key components are configured to be received from the single subset of users.

[0105] Example 37 includes the system of any of Examples 33-36, wherein the at least the second set of key components of the at least 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.

[0106] Example 38 includes the system of any of Examples 33-37, 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.

[0107] Example 39 includes the system of any of Examples 33-38, wherein the key is configured to include a one in each bit position where bits in a corresponding bit position in both the encrypted key and the at least one encryption key are different; wherein the key is configured to include a zero in each bit position where bits in the corresponding bit position in both the encrypted key and the at least one encryption key are the same.

[0108] Example 40 includes the system of any of Examples 33-39, wherein when the key needs to be used, the at least one processor is further configured to: erase the key from the at least one memory after use.

[0109] Example 41 includes the system of Example 40, wherein the at least one processor is configured to erase the key from the at least one memory after use using a DoD memory wipe.

[0110] Example 42 includes the system of any of Examples 33-41, wherein prior to reconstructing the key when the key needs to be generated, the at least one processor is configured to: block user logins into the system; verify that no users are logged into the system; and check that the system is not being implemented as a virtual machine.

[0111] Example 43 includes the system of Example 42, wherein the at least one processor is configured to block user logins into the system at least in part by being configured to: block secure shell (SSH) logins into the system.

[0112] Example 44 includes the system of any of Examples 33-43, further comprising at least one network interface communicatively coupled to the at least one processor and configured to communicate with external computing devices.

[0113] Example 45 includes the system of Example 44, wherein when the key needs to be used, the at least one processor is further configured to: cause a request for key components from to be communicated to users using the at least one network interface.

[0114] Example 46 includes the system of Example 45, wherein the request for key components is communicated to users using encrypted communication; wherein the first subset of the first key components is received from the first subset of users using encrypted communication; and wherein the at least the second subset of key components of the at least the second key components is received from the at least the second subset of users using encrypted communication.

[0115] Example 47 includes the system of any of Examples 45-46, 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, Wi-Fi, or near field (NFC) transmission.

[0116] Example 48 includes the system of any of Examples 33-47, wherein the first subset of users is the same subset of users as the second plurality of subsets of users.

[0117] Example 49 includes the system of any of Examples 33-48, 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.

[0118] Example 50 includes the system of any of Examples 33-49, wherein at least one of the key and the at least one encryption key is a private key used in asymmetrical cryptography.

[0119] Example 51 includes 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 set of key components from at least a subset of users that can be used to reconstruct an encrypted private key and at least one encryption key used to decrypt the private key from the encrypted private key; when the at least the one set of key components is received 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, 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.

[0120] Example 52 includes the system of Example 51, 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.

[0121] Example 53 includes the system of any of Examples 51-52, wherein the at least one processor is configured to: receive at least one set of key components from at least a subset of users that can be used to reconstruct an encrypted private key and 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 key components of at least 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 key from the encrypted 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 key components is received from the first subset of users, reconstruct the encrypted private key; and when the at least the second subset of key components of the at least the second key components is received from the at least the second subset of users, reconstruct the at least one encryption key.

[0122] Example 54 includes the system of Example 53, wherein the request for key components is communicated to users using encrypted communication; wherein the first subset of the first key components is received from the first subset of users using encrypted communication; and wherein the at least the second subset of key components of the at least the second key components is received from the at least the second subset of users using encrypted communication.

[0123] Example 55 includes the system of any of Examples 51-54, 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, Wi-Fi, or near field (NFC) transmission.

[0124] Example 56 includes the system of any of Examples 51-55, 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.

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 into a first set of first key components, wherein at least a first subset of the first set of first 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;

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 the second set of second key components.

3. The system of claim 1, wherein the at least the second set of 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.

4. The system of claim 1, 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 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 second key components to second external computing devices for the second plurality of users.

5. The system of claim 4, wherein at least one of the first set of first key components and the at least the second set of 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.

6. 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.

7. 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.

8. 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 the second set of second key components through at least one of polynomial interpolation or Shamir secret sharing.

9. 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 into a first set of first key components, wherein at least a first subset of the first set of first 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.

10. The system of claim 9, 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 the second set of second key components.

11. The system of claim 9, 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 the second set of second key components through at least one of polynomial interpolation or Shamir secret sharing.

12. 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 used that is encrypted as an encrypted key, the at least one processor is 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 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 first subset of the first set of first key components is received from the first subset of users that can be used to reconstruct the encrypted key, reconstruct the encrypted key;

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, 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.

13. The system of claim 12, wherein the at least the second set of 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.

14. The system of claim 12, 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.

15. The system of claim 12, 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.

16. The system of claim 15, 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.

17. The system of claim 12, wherein the first subset of users is the same subset of users as the second subset of users.

18. The system of claim 12, 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.

19. 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 a first subset of a first set of first key components from a first subset of users that can be used to reconstruct an encrypted private key;

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 first subset of the first set of first key components is received from the first subset of users that can be used to reconstruct the encrypted private key, reconstruct the encrypted private key;

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, reconstruct 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.

20. The system of claim 19, 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.

21. The system of claim 19, 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.