(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2018 (25.10.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/194634 A1

(51) International Patent Classification:
H04L 9/28 (2006.01) *H04L 12/22* (2006.01)

(21) International Application Number:
PCT/US2017/028737

(22) International Filing Date:
21 April 2017 (21.04.2017)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 11445 Compaq Center Drive W., Houston, Texas 77070 (US).

(72) Inventors: **MOHAMMAD, Nassir**; Filton Road Stoke Gifford, Pt., Bristol Bristol BS34 8QZ (GB). **GRIFFIN, Jonathan**; Filton Road Stoke Gifford, Pt., Bristol Bristol BS34 8QZ (GB). **GREWAL, Gurchetan**; Filton Road Stoke Gifford, Pt., Bristol Bristol BS34 8QZ (GB). **MATHER, Luke T.**; Filton Road Stoke Gifford, Pt., Bristol Bristol BS34 8QZ (GB). **SCHIFFMAN, Joshua Serratelli**; Filton Road Stoke Gifford, Pt., Bristol Bristol BS34 8QZ (GB).

(74) Agent: **BURROWS, Sarah** et al.; HP Inc., 3390 E. Harmony Road, Mail Stop 35, Fort Collins, Colorado 80528 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: ENCRYPTION KEY SHARES TO DIFFERENT DEVICES FOR RENDERING

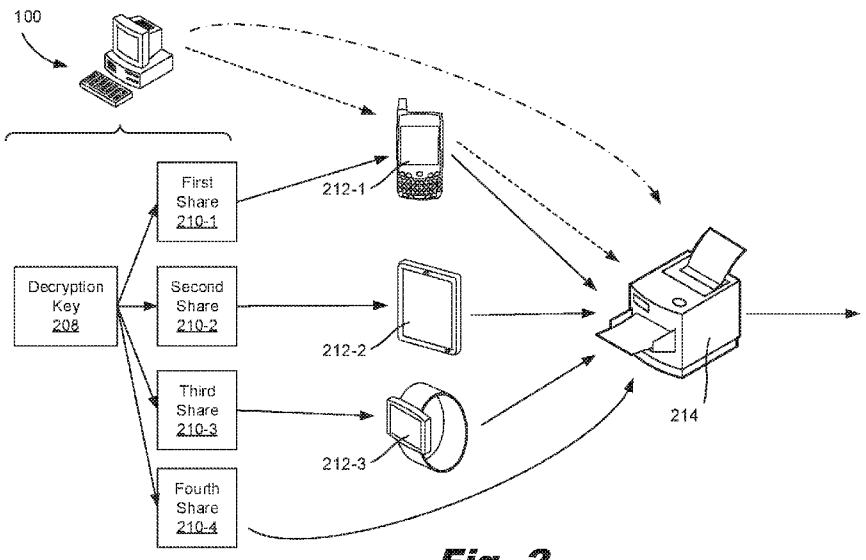

Fig. 2

(57) Abstract: In one example in accordance with the present disclosure, a computing device is described. The computing device includes an encryption device to encrypt, using an encryption key, a document to be rendered. A generating device generates multiple shares of a decryption key using a secret-sharing scheme. A threshold number of the multiple shares allows decryption of the document. A transmit device transmits different shares of the multiple shares to different devices. The document is rendered when the threshold number of multiple shares are rejoined at a rendering device.

WO 2018/194634 A1

[Continued on next page]

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

— *with international search report (Art. 21(3))*

ENCRYPTION KEY SHARES TO DIFFERENT DEVICES FOR RENDERING

BACKGROUND

[0001] In many facilities, such as office spaces or any number of public locations, community printers are disposed for use by multiple individuals. That is, users may have individual workstations for document creation. Once a document is created, it is sent to one such community printer for physical reproduction, which community printer serves various individuals. Such community systems have certain inefficiencies.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The accompanying drawings illustrate various examples of the principles described herein and are part of the specification. The illustrated examples are given merely for illustration, and do not limit the scope of the claims.

[0003] Fig. 1 is a block diagram of a computing device for transmitting decryption key shares to different devices for rendering, according to an example of the principles described herein.

[0004] Fig. 2 is a diagram of an environment of device for transmitting decryption key shares to different devices for rendering, according to an example of the principles described herein.

[0005] Fig. 3 is a flowchart of a method for transmitting decryption key shares to different devices for rendering, according to an example of the principles described herein.

[0006] Fig. 4 is a flowchart of a method for device for transmitting decryption key shares to different devices for rendering, according to another example of the principles described herein.

[0007] Fig. 5 is a diagram of a computing system to device for transmitting decryption key shares to different devices for rendering, according to an example of the principles described herein.

[0008] Throughout the drawings, identical reference numbers designate similar, but not necessarily identical, elements. The figures are not necessarily to scale, and the size of some parts may be exaggerated to more clearly illustrate the example shown. Moreover, the drawings provide examples and/or implementations consistent with the description; however, the description is not limited to the examples and/or implementations provided in the drawings.

DETAILED DESCRIPTION

[0009] In many facilities, such as office spaces or any number of public locations, community printers are disposed for use by multiple individuals. That is, users may have individual workstations for document creation. Once a document is created, it is sent to one such community printer for physical reproduction, which community printer serves various individuals. However, such community systems may not provide a desired level of security or privacy.

[0010] For example, after sending a print job to a printer to be printed, a user may forget to retrieve the document, which may then sit on the printer, viewable to anyone who passes by. In another example, a different user may inadvertently pick up a document from a printer believing it belongs to them, or may inadvertently grab the subject print job along with their own. Such scenarios can lead to a breach of security and/or confidentiality if documents are of a sensitive nature.

[0011] Security can be increased by encrypting a document. In this case, following a transmittal of the encrypted document to a printer or printing, a user associated with the print job goes to the printer and enters a password with which the document is decrypted. The document is then decrypted and printed.

However, these systems as well are subject to security breaches. That is, a username and password are not cryptographically strong and can be broken with relative ease, for example through brute force techniques. Moreover, with the proliferation of technological devices, users have many different usernames and passwords and adding one more to that already long list may make a user less likely to remember a print job username and password.

[0012] Accordingly, the present specification describes systems and methods that overcome these and other complications. Specifically, a document may be encrypted and passed to a printing device. In some examples, the encryption may rely on a symmetric encryption key, meaning the key to encrypt the document and the key to decrypt the document are the same. In other examples, the encryption may be asymmetric, meaning the key to encrypt the document is different from the key to decrypt the document.

[0013] Through a secret-sharing scheme, multiple shares of the decryption key may be generated. Each of the shares may be passed to a different device. As a user is standing in front of the printing device, a certain number of those shares presented at the rendering device allow the document to be decrypted and printed. If any amount of shares less than the threshold number are presented, the document is not decrypted.

[0014] Specifically, the present specification describes a computing device. The computing device includes an encryption device to encrypt a document to be rendered using an encryption key. A generating device, using a secret-sharing scheme, generates multiple shares of a decryption key such that a threshold number of the multiple shares allow decryption of the document. A transmit device of the computing device transmits different shares of the multiple shares to different devices. In this example, the document is rendered when the threshold number of multiple shares are rejoined at a rendering device.

[0015] The present specification also describes a method of transmitting decryption key shares to different devices for document rendering. According to the method, a document to be rendered is encrypted using an encryption key. Using a secret-sharing scheme, multiple shares are generated from a

decryption key such that a threshold number of the multiple shares allow reconstruction of the document. The different shares are then transmitted to different devices. The document is rendered when the threshold number of the multiple shares are rejoined at a rendering device.

[0016] The present specification also describes a computing system. The computing system includes a processor and a machine-readable storage medium coupled to the processor. An instruction set stored in the machine-readable storage medium is executed by the processor. The instruction set includes instructions to encrypt a document to be printed using an encryption key, instructions to generate, using a secret-sharing scheme, multiple shares of a decryption key, wherein a rejoining of a threshold number of the multiple shares allows decryption of the document, and instructions to transmit different shares of the multiple shares to different devices. The document is rendered when the threshold number of multiple shares are rejoined at a printer.

[0017] In summary, using such a computing device 1) allows for print job security by requiring multiple devices, each having different shares of a decryption key, to be present at a printer before a document can be printed or otherwise rendered; 2) avoids a cumbersome username and password entry; and 3) relies on multiple user devices, which may be on a person, during print job authorization. However, it is contemplated that the devices disclosed herein may address other matters and deficiencies in a number of technical areas.

[0018] As used in the present specification and in the appended claims, the term "rendering device" refers to a device that renders, either digitally or physically a document or other image. Examples of rendering devices include digital displays, printers, or other devices.

[0019] Further, as used in the present specification and in the appended claims, the term "a number of" or similar language is meant to be understood broadly as any positive number including 1 to infinity.

[0020] Turning now to the figures, Fig. 1 is a block diagram of a computing device (100) for transmitting decryption key shares to different devices for rendering, according to an example of the principles described herein. The

computing device (100) may be any electronic device that can receive and/or generate a document to be rendered in either a digital or a physical format. Examples of such computing devices (100) include desktop computers, laptop computers, tablets, scanners, and personal digital assistants, among others.

[0021] The computing device (100) includes an encryption device (102) that encrypts a document to be rendered. Such encryption can be either symmetric or asymmetric. In symmetric encryption, the encryption key and decryption key are the same. In asymmetric encryption, the encryption key is different from the decryption key. A key is a random string of bits that is used to scramble the information in the document to be rendered. Upon reception at a rendering device, the decryption key is used to decrypt, or unscramble, the document such that it is legible and ready for rendering. As the decryption key is the vehicle by which an encrypted document is accessible, it may be desirable to decrease the likelihood of inadvertent/malicious unauthorized access to the decryption key.

[0022] Accordingly, a generate device (104) of the computing device (100), generates, from a secret-sharing scheme, multiple shares of the decryption key. Secret sharing refers to the distribution of a key amongst a group of participants, each of whom is allocated a share of the key. The key is reconstructed when a sufficient number, of possibly different types, of shares are combined together. That is, an individual share of the key, by itself is ineffective. In one type of secret sharing scheme, a share of the key is given to a number of recipients, and the key will be reconstructed from their shares when specific conditions are fulfilled. For example, the shares may be distributed to each recipient such that that a threshold number of recipients can together reconstruct the key, but no group of less than the threshold number can reconstruct the key. Doing so increases the security provided by an encryption as these different shares are distributed and reduce the likelihood of an attacker/entity collecting enough shares to reconstruct the decryption key. That is, the decryption key security is increased as it is a distributed key, thus reducing the likelihood that an entity will be able to acquire the portions used to decrypt a document.

[0023] As described, a threshold number of these multiple shares, when rejoined, will allow for a decryption of the document. Note that the threshold number may be less than the total number of shares. That is of the four shares, rejoining three may be sufficient to decrypt the document. However, if the threshold number is three, then the rejoining of two shares will not facilitate a decryption, and subsequent release of the print job.

[0024] A transmit device (106) of the computing device (100) transmits the different shares of the multiple shares to different devices. In some cases, the different devices include at least a rendering device on which the document is to be rendered and at least one other device. Sending at least one of the shares to the rendering device increases print job security as the print job is decrypted when the particular printing device on which it is to be printed participates in key reconstruction. In other examples, the different devices do not include a rendering device, i.e., printer, to which the document is to be rendered.

[0025] In either case, the devices that are not rendering devices may correspond to a single user. For example, a first share of the decryption key could be sent to the rendering device on which the document is to be rendered, a second share could be sent to a network-connected watch of the user, and a third share could be sent to a network-connected mobile device of the user. As described above, such a system enhances rendering security, as a breach of just one of the aforementioned devices will not be sufficient to allow decryption and access of the document.

[0026] In another example, the different devices may correspond to different users. That is a first share of the decryption key may be sent to a first user's mobile device and a second share of the decryption key may be sent to a second user's mobile device. Accordingly, the document is decrypted and rendered when at least the first user and the second user, and their corresponding devices, are present at the rendering device. In so doing, a rejoin engine recombines the various shares of the decryption key, responsive to there being more than the threshold number of various shares present at the rendering device.

[0027] Such a system allows for increased security in document rendering. That is, even if all of the multiple devices are stolen or successfully attacked, the document is not exposed because they do not have enough shares between them to decrypt the document. Until the multiple devices are present at the rendering device, there is not enough information on the rendering device to decrypt the document, even in the case where the encrypted document is sent directly to the rendering device. The unencrypted document exists for a short while on the rendering device, as it can be decrypted, rendered, and then deleted.

[0028] Fig. 2 is a diagram of an environment of transmitting decryption key shares (210) to different devices (212) for rendering, according to an example of the principles described herein. As described above, a computing device (100) uses an encryption key to encrypt a document such that the document is accessible in a decrypted format to just an authorized entity. As described above the decryption key (208) associated with the encryption key may be used to generate multiple shares (210). While Fig. 2 depicts a first share (210-1), a second share (210-2), a third share (210-3), and a fourth share (210-4), the decryption key (208) may be divided into any number of sections (210). Note that in Fig. 2, the transmission of the decryption key (208) and its corresponding shares (210) are indicated by solid arrows, while transmission of an encrypted document is indicated by dashed arrows and dashed-dot arrows.

[0029] These shares can then be passed to different devices (212). This may occur without additional user input above selecting to render a document. For example, upon selecting a "Print" button on the computing device (100), the decryption key (208) may be divided into shares (210) and the shares (210) passed to the various devices (212). Specifically, a first share (210-1) may be sent to a first device (212-1). Similarly, a second share (210-2) and a third share (210-3) may be sent to a second device (212-2) and a third device (212-3), respectively. Note again, that as described above, each of the different devices (212) may correspond to one user or to multiple users.

[0030] In addition to sending different shares (210) to different devices (212), in some examples, at least one of the shares (210) can be sent directly to the

rendering device (214). That is, in addition to receiving the encrypted document, the rendering device (214), such as a printer, may receive a fourth share (210-4). Accordingly, a malicious entity would not only have to acquire the devices (212) on which shares (210) of the decryption key (208) are stored, but would also have to be physically present at the rendering device (214) to acquire a sufficient number of shares (210) to facilitate document decryption.

[0031] When the threshold number of shares (210) have been presented at the rendering device (214), they may be rejoined, for example by a rejoin engine, and the document decrypted and/or rendered. In some examples, the shares (210) may be communicated to the rendering device (214) via an encrypted network. That is, a user may establish a secured connection, over a secured authenticated channel, for example a short-range network, which may occur previous to such rendering or at the same time as such rendering. Accordingly, when the devices (212) are within a predetermined proximity, the rendering device (214) can acquire the shares (210) to begin rejoining of the decryption key (208) at the rendering device (214).

[0032] Note that in Fig. 2 the transmission of the document, as indicated by the dashed and dashed-dot line is separate from the transmission of the entire decryption key (208). Doing so enhances security as hacking a device that includes the encrypted document will not necessarily result in a hacking of the entire decryption key (208), but at most a share (210), which share (210) by itself does not allow for decryption of the encrypted document.

[0033] In some examples, the computing device (100), in addition to transmitting the decryption key shares (210) to various devices (212), may transmit the encrypted document. In one example, the encrypted document is transmitted to at least one of the devices (212), in this example, a first device (212-1). Then, when in proximity to the rendering device (214), the encrypted document, in addition to the first share (210-1) of the decryption key (208) can be passed to the rendering device (214) for decrypting.

[0034] In another example, the computing device (100) transmits the encrypted document directly to the rendering device (214), i.e., the printer. Doing so ensures that any device (212) which may have access to a share

(210) of the decryption key (208) will not have access to the document intended to be decrypted with the decryption key (208).

[0035] Fig. 3 is a flowchart of a method (300) for transmitting decryption key shares (Fig. 2, 210) to different devices (Fig. 2, 212) for rendering, according to an example of the principles described herein. As a general note, the methods (300, 400) may be described below as being executed or performed by at least one device, for example, the computing device (Fig. 1, 100). Other suitable systems and/or computing devices may be used as well. The methods (300, 400) may be implemented in the form of executable instructions stored on at least one machine-readable storage medium of at least one of the devices and executed by at least one processor of at least one of the device. Alternatively, or in addition, the methods (300, 400) may be implemented in the form of electronic circuitry (e.g., hardware). While Figs. 3 and 4 depict operations occurring in a particular order, a number of the operations of the methods (300, 400) may be executed concurrently or in a different order than shown in Figs. 3 and 4. In some examples, the methods (300, 400) may include more or less operations than are shown in Figs. 3 and 4. In some examples, a number of the operations of the methods (300, 400) may, at certain times, be ongoing and/or may repeat. Include questions as you come up with them

[0036] According to the method (300), a document to be rendered is encrypted (block 301) using an encryption key. The encryption key may be a random string of bits that is used to scramble a document such that it is illegible, or inaccessible to inadvertent or malicious access. As described above, the encryption key may be the same as or different than the decryption key

[0037] The decryption key (Fig. 2, 208) is then used in a secret-sharing scheme to generate (block 302) multiple shares (Fig. 2, 210). The divided shares (Fig. 2, 210) when rejoined allow the decrypting of the associated document. Generating (block 302) these decryption key (Fig. 2, 208) shares (Fig. 2, 210) increases the security of the rendering operation. That is, a malicious user would have to acquire multiple of these different shares (Fig. 2, 210) before being able to access the associated document, which may be encrypted due to sensitive or confidential reasons.

[0038] The different shares (Fig. 2, 210) are then transmitted (block 303) to different devices (Fig. 2, 212). For example, the different shares (Fig. 2, 210) may be transmitted (block 303) to different devices (Fig. 2, 212) corresponding to a single user such that, to decrypt a document, a user would present a threshold number of those different shares (Fig. 2, 210) at the rendering device (Fig. 2, 214).

[0039] Note that in some examples the devices (Fig. 2, 212) to which the different shares (Fig. 2, 210) are sent may include the rendering device (Fig. 2, 214). A specific example of this scenario is now provided. In this example, a first share (Fig. 2, 210-1) may be passed to a mobile device (Fig. 2, 212-1) of a user. Similarly, a second share (Fig. 2, 210-2) and a third share (Fig. 2, 210-3) may be sent to a tablet device (Fig. 2, 212-2) and a smart watch device (Fig. 2, 212-3) both corresponding to the same user. A fourth share (Fig. 2, 210-4) may be sent to the rendering device (Fig. 2, 214) itself. In this example, the threshold number of shares (Fig. 2, 210) for decrypting the document is three. Accordingly, if the user, wearing the smart watch device (Fig. 2, 212-3) approaches the rendering device (Fig. 2, 214), and establishes a secure connection, the user may not be permitted to decrypt the document as there are less than the threshold amount of shares (Fig. 2, 210) presented, one from the rendering device (Fig. 2, 214) and one from the smart watch device (Fig. 2, 212-3).

[0040] By comparison, if the user, wearing a smart watch device (Fig. 2, 212-3) and carrying a mobile device (Fig. 2, 212-1) approaches the rendering device (Fig. 2, 214), and establishes a secure connection, the user may be permitted to decrypt the document as there are now the threshold three shares (Fig. 2, 210), one from the rendering device (Fig. 2, 214), one from the smart watch device (Fig. 2, 212-3), and one from the mobile device (Fig. 2, 212-1). As has been demonstrated, such action reduces the likelihood that a decryption key, and thereby an encrypted document, will fall into malicious hands.

[0041] In another example, the different shares (Fig. 2, 210) are transmitted (block 303) to devices (Fig. 2, 212) corresponding to different users. In this example, a first share (Fig. 2, 210-1) may be passed to a mobile device (Fig. 2,

212-1) belonging to a first user. A second share (Fig. 2, 210-2) may be passed to a tablet device (Fig. 2, 212-2) belonging to a second user and a third share (Fig. 2, 210-3) may be passed to a smart watch device (Fig. 2, 212-3) belonging to a third user. A fourth share (Fig. 2, 210-4) may be sent to the rendering device (Fig. 2, 214) itself. In this example, the threshold number of shares (Fig. 2, 210) for decrypting the document is three. Accordingly, if the first user with their mobile device (Fig. 2, 212-1) approaches the rendering device (Fig. 2, 214), and establishes a secure connection, the user may not be permitted to decrypt the document as there less than the threshold number of shares (Fig. 2, 210) presented, one from the rendering device (Fig. 2, 214) and one from the mobile device (Fig. 2, 212-1).

[0042] By comparison, if the first user with the mobile device (Fig. 2, 212-1) and the second user with the tablet device (Fig. 2, 212-2) approach the rendering device (Fig. 2, 214), and establishes a secure connection, the users may be permitted to decrypt the document as there are now the threshold three shares (Fig. 2, 210), one from the rendering device (Fig. 2, 214), one from the tablet device (Fig. 2, 212-2), and one from the mobile device (Fig. 2, 212-1). As has been demonstrated, such action reduces the likelihood that a decryption key, and thereby an encrypted document, will fall into malicious hands.

[0043] Fig. 4 is a flowchart of a method (400) for transmitting decryption key shares (Fig. 2, 210) to different devices (Fig. 2, 212) for rendering, according to another example of the principles described herein. According to the method (400), different devices (Fig. 2, 212) to which the shares (Fig. 2, 210) are transmitted are selected (block 401). This may be performed by a managing entity such as a network administrator, employer, etc. via a management computing device. For example, an employer may set a user profile wherein it is determined what devices (Fig. 2, 212) for that user will receive shares (Fig. 2, 210) of a decryption key (Fig. 2, 208) used by that user and which, if any devices (Fig. 2, 212) for other users will receive shares (Fig. 2, 210) of the decryption key (Fig. 2, 208). Each subsequent document encryption/decryption can then follow the settings in this user profile. The document is then encrypted (block 402) as described above in connection with Fig. 3. That is an encryption

device (Fig. 1, 102) of a computing device (Fig. 1, 100) encrypts (block 402) the document.

[0044] From the decryption key (Fig. 2, 208) a set of shares (Fig. 2, 210) can be generated (block 403). That is a generate device (Fig. 1, 104) of a computing device (Fig. 1, 100) generates (block 403) a set of shares (Fig. 2, 210). A threshold number of shares (Fig. 2, 210) will be needed to rejoin the different portions of the decryption key (Fig. 2, 208). A specific example of share generation (block 403) is now provided. In this example, assuming there are ***D***, number of devices (Fig. 2, 212), a secret-sharing policy may indicate that a threshold number of devices, ***P***, should be present at a rendering device (Fig. 2, 214) to allow rejoinment of the shares (Fig. 2, 210), which threshold number of devices, ***P***, is less than ***D***. A number of shares, ***N***, are then generated (block 403) using a secret-sharing scheme that indicates a threshold number of shares, ***K***, which should be present at the rendering device (Fig. 2, 214) to allow rejoinment of the shares (Fig. 2, 210), and decryption of the document. As a specific example, the threshold number of shares, ***K***, may be defined as $K = N/2 + P$.

[0045] In this example, A first portion of the shares (Fig. 2, 210), i.e., the first portion defined as the first $N/2$ shares (Fig. 2, 210), are distributed evenly amongst the ***D*** devices (Fig. 2, 212) and the remaining shares (Fig. 2, 210), a second portion defined as a second set of $N/2$ shares (Fig. 2, 210), are distributed to the rendering device (Fig. 2, 214). Doing so ensures 1) that at least ***P*** devices and a rendering device (Fig. 2, 214) are present to allow decryption of the document, 2) that all the devices (Fig. 2, 212) together don't have enough shares (Fig. 2, 210) to decrypt the document; and that even if there are multiple rendering devices (Fig. 2, 214) and all are attacked, they cannot decrypt the document without ***P*** devices (Fig. 2, 212) being present as well.

[0046] The different shares (Fig. 2, 210) are then transmitted (block 404) to the different devices (Fig. 2, 212). That is a transmit device (Fig. 1, 106) of a computing device (Fig. 1, 100) transmits (block 404) the shares (Fig. 2, 210) to the different devices. This may be performed as described above in regards to

Fig. 3. This type of sharing easily ensures that even all the non-rendering devices cannot reconstruct the decryption key together, nor can the rendering device (Fig. 2, 214).

[0047] By so doing, rendering security is even further increased. That is, a malicious entity would have to hack a first number of devices (Fig. 2, 212) and a rendering device (Fig. 2, 214) to obtain sufficient shares (Fig. 2, 210) to decrypt the document. The encrypted document can also be transmitted (block 405) to at least one of the devices (Fig. 2, 212). This may be performed as described above in regards to Fig. 2.

[0048] According to the method (400), the decryption and rendering of the document is prevented (block 406) until a threshold number of shares (Fig. 2, 210) have been rejoined. For example, as described above, if a threshold number of shares (Fig. 2, 210) for a particular document is set to three, the system would prevent decryption and rendering until more shares (Fig. 2, 210) are rejoined at the rendering device (Fig. 2, 214).

[0049] Fig. 5 is a diagram of a computing system (516) to transmitting decryption key shares (Fig. 2, 210) to different devices (Fig. 2, 212) for rendering, according to an example of the principles described herein. To achieve its desired functionality, the computing system (516) includes various hardware components. Specifically, the computing system (516) includes a processor (518) and a machine-readable storage medium (520). The machine-readable storage medium (520) is communicatively coupled to the processor (518). The machine-readable storage medium (520) includes a number of instruction sets (522, 524, 526) for performing a designated function. The machine-readable storage medium (520) causes the processor (518) to execute the designated function of the instruction sets (522, 524, 526).

[0050] Although the following descriptions refer to a single processor (518) and a single machine-readable storage medium (520), the descriptions may also apply to a computing system (516) with multiple processors and multiple machine-readable storage mediums. In such examples, the instruction sets (522, 524, 526) may be distributed (e.g., stored) across multiple machine-readable storage

mediums and the instructions may be distributed (e.g., executed by) across multiple processors.

[0051] The processor (518) may include at least one processor and other resources used to process programmed instructions. For example, the processor (518) may be a number of central processing units (CPUs), microprocessors, and/or other hardware devices suitable for retrieval and execution of instructions stored in machine-readable storage medium (520). In the computing system (516) depicted in Fig. 5, the processor (518) may fetch, decode, and execute instructions (522, 524, 526) for detecting failing components in a device. In one example, the processor (518) may include a number of electronic circuits comprising a number of electronic components for performing the functionality of a number of the instructions in the machine-readable storage medium (520). With respect to the executable instruction, representations (e.g., boxes) described and shown herein, it should be understood that part or all of the executable instructions and/or electronic circuits included within one box may, in alternate examples, be included in a different box shown in the figures or in a different box not shown.

[0052] The machine-readable storage medium (520) represent generally any memory capable of storing data such as programmed instructions or data structures used by the computing system (516). The machine-readable storage medium (520) includes a machine-readable storage medium that contains machine-readable program code to cause tasks to be executed by the processor (518). The machine-readable storage medium (520) may be tangible and/or non-transitory storage medium. The machine-readable storage medium (520) may be any appropriate storage medium that is not a transmission storage medium. For example, the machine-readable storage medium (520) may be any electronic, magnetic, optical, or other physical storage device that stores executable instructions. Thus, machine-readable storage medium (520) may be, for example, Random Access Memory (RAM), a storage drive, an optical disc, and the like. The machine-readable storage medium (520) may be disposed within the computing system (516), as shown in Fig. 5. In this situation, the executable instructions may be "installed" on the computing system (516). In

one example, the machine-readable storage medium (520) may be a portable, external or remote storage medium, for example, that allows the computing system (516) to download the instructions from the portable/external/remote storage medium. In this situation, the executable instructions may be part of an "installation package". As described herein, the machine-readable storage medium (520) may be encoded with executable instructions for dividing an encryption key (Fig. 2, 208) to different devices (Fig. 2, 212) for rendering.

[0053] Referring to Fig. 5, encrypt instructions (522), when executed by a processor (518), may cause the computing system (516) to encrypt a document to be printed using an encryption key. Generate instructions (524), when executed by a processor (518), may cause the computing system (516) to generate, using a secret-sharing scheme, multiple shares (Fig. 2, 210) of a decryption key (Fig. 2, 208). A rejoining of a threshold number of the multiple shares (Fig. 2, 210) for the decryption key (Fig. 2, 208) allows decryption of the document. Transmit instructions (526), when executed by a processor (518), may cause the computing system (516) to transmit different shares (Fig. 2, 210) of the multiple shares (Fig. 2, 210) to different devices (Fig. 2, 212). The document is rendered when the threshold number of the multiple shares (Fig. 2, 210) for the decryption key (Fig. 2, 208) are rejoined at a printer.

[0054] In some examples, the processor (518) and machine-readable storage medium (520) are located within the same physical component, such as a server, or a network component. The machine-readable storage medium (520) may be part of the physical component's main memory, caches, registers, non-volatile memory, or elsewhere in the physical component's memory hierarchy. In one example, the machine-readable storage medium (520) may be in communication with the processor (518) over a network. Thus, the computing system (516) may be implemented on a user device, on a server, on a collection of servers, or combinations thereof.

[0055] The computing system (516) of Fig. 5 may be part of a general-purpose computer. However, in some examples, the computing system (516) is part of an application specific integrated circuit.

[0056] In summary, using such a computing device 1) allows for print job security by requiring multiple devices, each having different sections of an encryption key, to be present at a printer before a document can be printed or otherwise rendered; 2) avoids a cumbersome username and password entry; and 3) relies on multiple user devices, which may be on a person, during print job authorization. However, it is contemplated that the devices disclosed herein may address other matters and deficiencies in a number of technical areas.

[0057] The preceding description has been presented to illustrate and describe examples of the principles described. This description is not intended to be exhaustive or to limit these principles to any precise form disclosed. Many modifications and variations are possible in light of the above teaching.

CLAIMS

WHAT IS CLAIMED IS:

1. A computing device comprising:

an encryption device to encrypt a document to be rendered using an encryption key;

a generating device to, using a secret-sharing scheme, generate multiple shares of decryption key such that a threshold number of the multiple shares allow decryption of the document; and

a transmit device to transmit different shares of the multiple shares to different devices, wherein the document is rendered when the threshold number of the multiple shares are rejoined at a rendering device.

2. The computing device of claim 1, wherein the multiple shares are receivable at a rendering device when within a predetermined proximity of the rendering device.

3. The computing device of claim 1, further comprising a rejoin engine to rejoin various shares of the multiple shares, wherein responsive to a number of rejoined shares being greater than the threshold number, the document is decrypted.

4. The computing device of claim 1, wherein the transmit device transmits the encrypted document to the rendering device which is decrypted when the threshold number of shares are rejoined at the rendering device.

5. A method comprising:

encrypting a document to be rendered using an encryption key;

generating multiple shares of a decryption key using a secret-sharing scheme such that a threshold number of the multiple shares allow reconstruction of the document; and

transmitting different shares of the multiple shares to different devices, wherein the document is rendered when the threshold number of the multiple shares are rejoined at a rendering device.

6. The method of claim 5, wherein the different devices comprise at least:

the rendering device on which the document is to be rendered; and

one other device.

7. The method of claim 5, wherein the different devices correspond to different users.

8. The method of claim 5, further comprising transmitting the encrypted document to at least one of the different devices.

9. The method of claim 5, further comprising selecting, before the encryption of the document, the different devices to which the multiple shares are to be transmitted.

10. The method of claim 5, further comprising preventing the decryption and rendering of the document until the threshold number of multiple shares have been rejoined.

11. The method of claim 5, wherein the threshold number of the multiple shares is less than a total number of multiple shares.

12. A computing system comprising:

a processor;

a machine-readable storage medium coupled to the processor; and

an instruction set, the instruction set being stored in the machine-readable storage medium to be executed by the processor, wherein the instruction set comprises:

instructions to encrypt a document to be printed using an encryption key;

instructions to generate, using a secret-sharing scheme, multiple shares of a decryption key, wherein a rejoining of a threshold number of the multiple shares key allows decryption of the document; and

instructions to transmit different shares of the multiple shares to different devices.

13. The computing system of claim 12, wherein a first set of shares are transmitted to non-rendering devices and a second set of shares are distributed to a rendering device.

14. The computing system of claim 13, wherein the threshold number of shares to allow decryption of the document includes shares from the first set of shares and shares from the second set of shares.

15. The computing system of claim 13, wherein:

the first set of shares are distributed among all of the non-rendering devices; and

the threshold number of multiple shares is such that a subset of all of the non-rendering devices and the rendering device allow rejoinment of the decryption key.

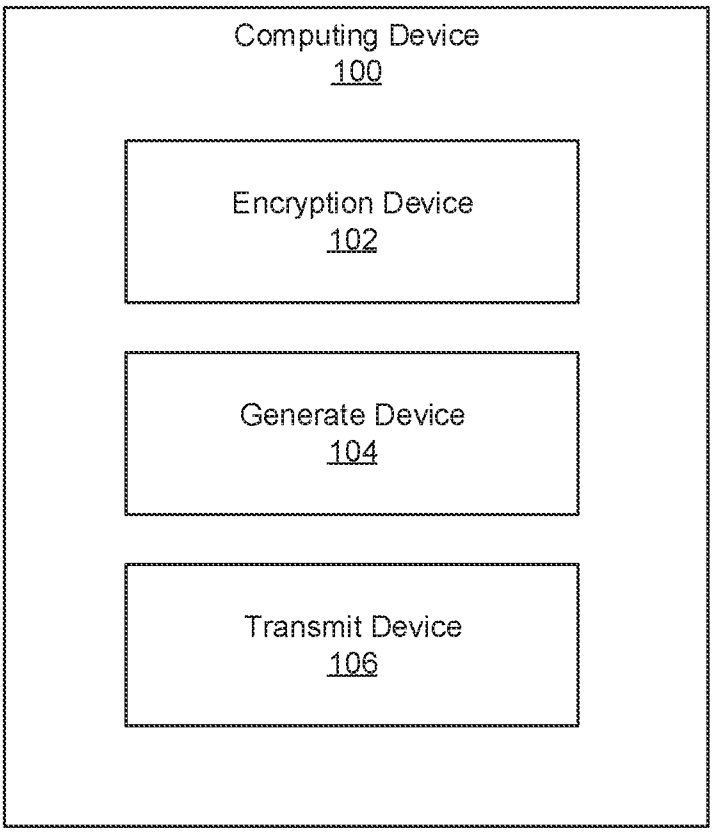
Computing Device
100
Encryption Device
102
Generate Device
104
Transmit Device
106

Fig. 1

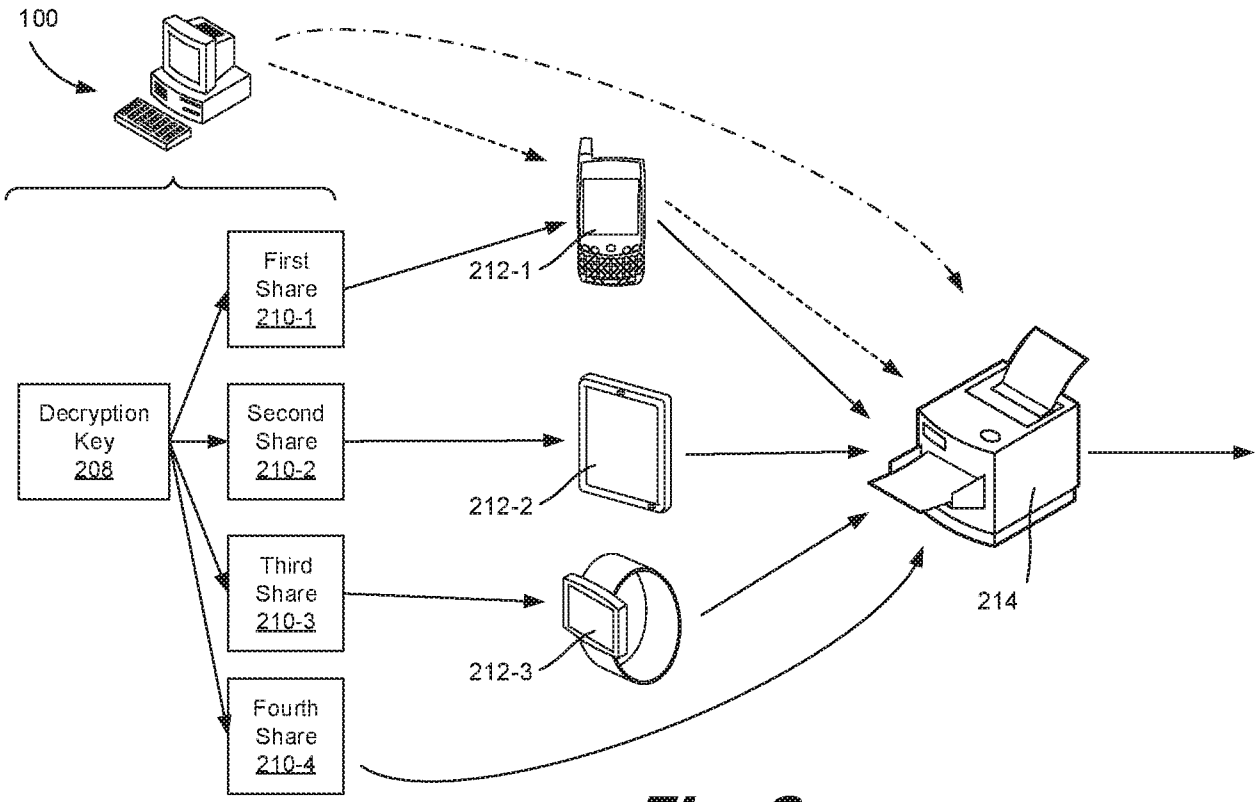
100
Decryption Key 208
First Share 210-1
Second Share 210-2
Third Share 210-3
Fourth Share 210-4
212-1
212-2
212-3
214

Fig. 2

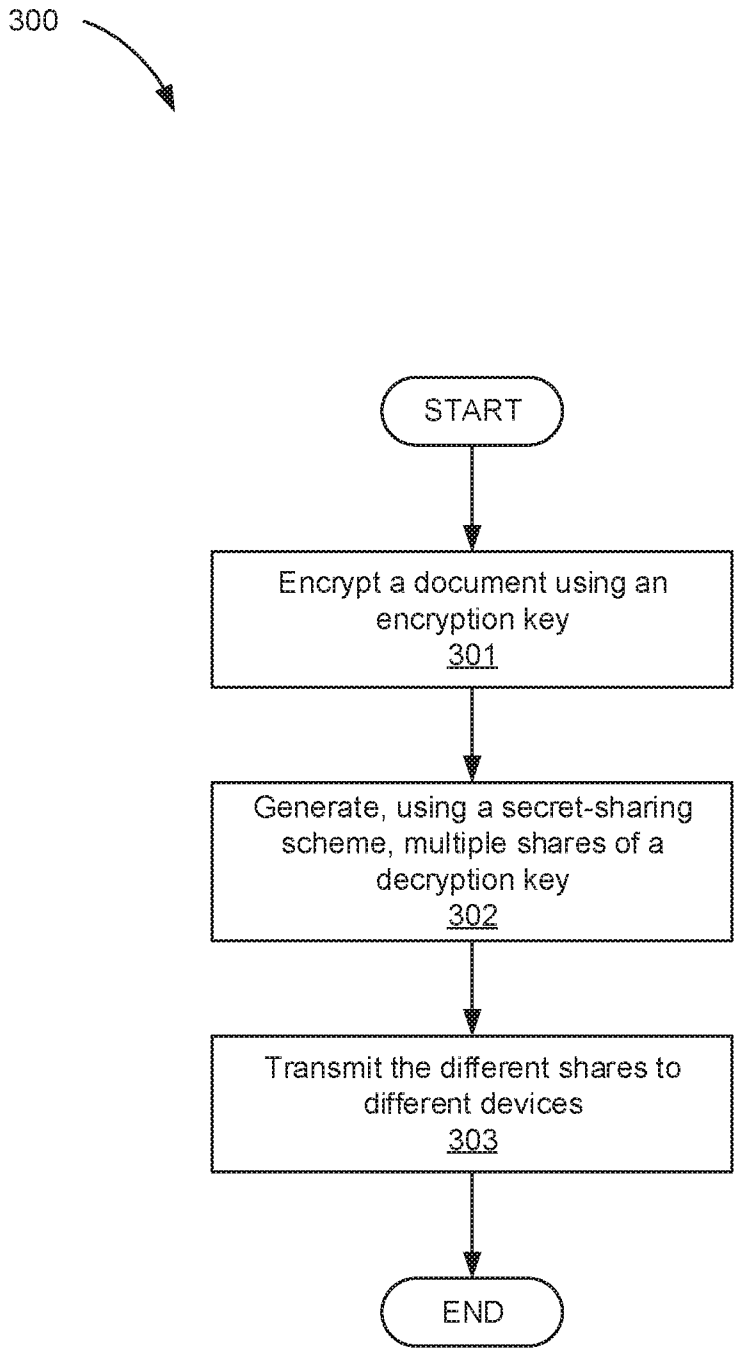
300
START
Encrypt a document using an encryption key
301
Generate, using a secret-sharing scheme, multiple shares of a decryption key
302
Transmit the different shares to different devices
303
END

Fig. 3

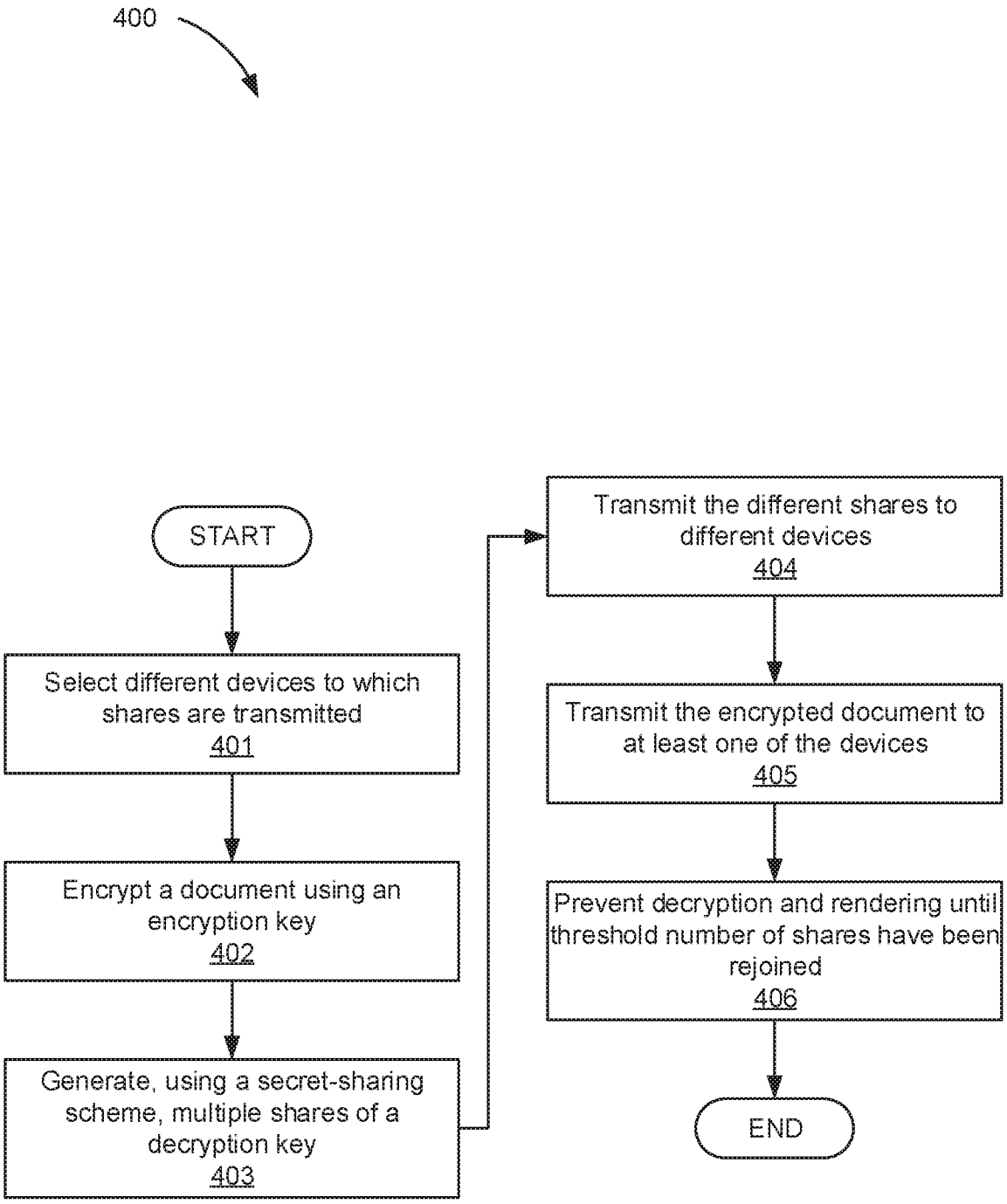
400
START
Select different devices to which shares are transmitted
401
Encrypt a document using an encryption key
402
Generate, using a secret-sharing scheme, multiple shares of a decryption key
403
Transmit the different shares to different devices
404
Transmit the encrypted document to at least one of the devices
405
Prevent decryption and rendering until threshold number of shares have been rejoined
406
END

Fig. 4

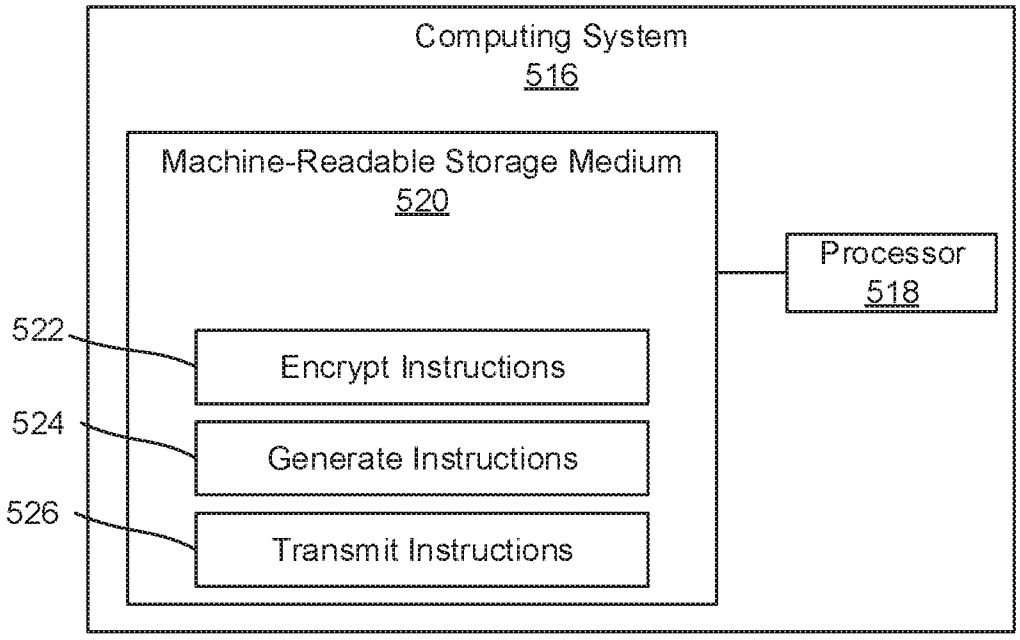
Computing System
516
Machine-Readable Storage Medium
520
Processor
518
522
Encrypt Instructions
524
Generate Instructions
526
Transmit Instructions

Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2017/028737

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/28 *(2006.01)*
H04L12/22 *(2006.01)*

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/00-9/32, 12/00-12/22, G06F 1/00-1/32, 21/00-21/72, H04W 12/00-12/04

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DWPI, ESP@cenet, K-PION, PAJ, PatSearch, RUPTO, USPTO, WIPO

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008263363 A1 (SPYRUS, INC.) 23.10.2008, paragraphs [0029]-[0035], [0037]-[0040], [0054]-[0058], [0061], [0065], [0067]-[0073], [0076]-[0077], [0086]-[0088], [0090]-[0092], [0099]-[0101], [0111]-[0117], [0171], [0178]	1-15
A	US 2002178354 A1 (CRAIG L. OGG et al.) 28.11.2002	1-15
A	US 7536547 B2 (OCE-TECHNOLOGIES B.V.) 19.05.2009	1-15
A	US 9594698 B2 (DELL PRODUCTS, LP) 14.03.2017	1-15

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 February 2018 (01.02.2018)	07 February 2018 (07.02.2018)

Name and mailing address of the ISA/RU:
Federal Institute of Industrial Property,
Berezhkovskaya nab., 30-1, Moscow, G-59,
GSP-3, Russia, 125993
Facsimile No: (8-495) 531-63-18, (8-499) 243-33-37

Authorized officer

I.Belikov

Telephone No. (8-495) 531-65-15