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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 March 2017 (16.03.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/044110 A1

(51) International Patent Classification:
G11C 11/15 (2006.01)

(21) International Application Number:
PCT/US2015/049572

(22) International Filing Date:
11 September 2015 (11.09.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, TX 77070 (US).

(72) Inventors: **KIM, Kyung Min**; 1501 Page Mill Road, Palo Alto, California 94304 (US). **GE, Ning**; 1501 Page Mill Road, Palo Alto, California 94304 (US). **WILLIAMS, R. Stanley**; 1501 Page Mill Road, Palo Alto, California 94304 (US). **LI, Zhiyong**; 1501 Page Mill Road, Palo Alto, California 94304 (US).

(74) Agents: **ZHANG, Shu** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, CO 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, 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, KN, KP, KR, 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, 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))*

WO 2017/044110 A1

(54) Title: SECURING DATA WITH MEMRISTORS

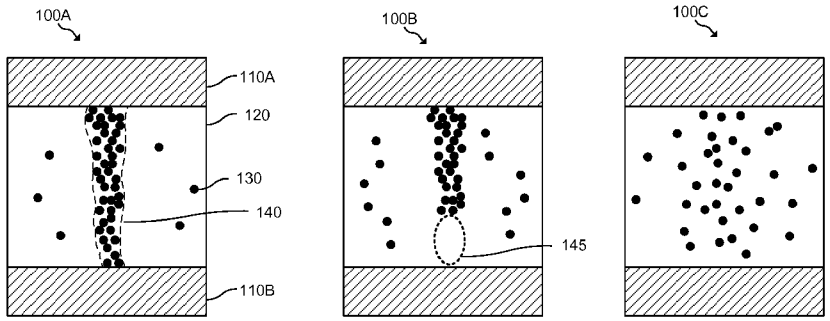

FIG. 1

(57) Abstract: Example embodiments relate to securing data with memristors. The examples disclosed herein provide a memristor where the memristor is in one of a first resistance state and a second resistance state. An encryption is applied to the memristor to tune the memristor to a third resistance state. The encryption determines a decryption voltage that tunes the memristor from the third resistance state to its original state.

SECURING DATA WITH MEMRISTORS

BACKGROUND

[0001] Data encryption utilizes a specific encryption key to encode data for generating secured data. A decryption key is used to decode the secured data. The encryption key and the decryption key is confidentially synchronized.

[0002] Memristors are devices that can be programmed to different resistive states by applying a programming energy, such as a voltage or current. Memory devices with memristors can be used in a variety of applications, including memory, programmable logic, signal-processing control systems, pattern recognition, and other applications.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The following detailed description references the drawings, wherein:

[0004] FIG. 1 is a diagram of cross-sectional views of an example memristor in a first resistance state, a second resistance state, and a third resistance state;

[0005] FIG. 2 is a block diagram of an example system for securing data with memristors;

[0006] FIG. 3A is a schematic diagram showing a cross-sectional view of an example memristor being tuned by an encryption;

[0007] FIG. 3B is a schematic diagram showing a cross-sectional view of an example memristor being tuned by a decryption voltage;

[0008] FIG. 4A is a flowchart of an example method for securing data with a memristor;

[0009] FIG. 4B is a flowchart of an example method for securing data with a memristor including decrypting secured data; and

[0010] FIG. 4C is a flowchart of an example method for securing data with a memristor including decrypting secured data including determining the original state of the memristor.

DETAILED DESCRIPTION

[0011] The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description to refer to the same or similar parts. While several examples are described in this document, modifications, adaptations, and other implementations are possible. Accordingly, the following detailed description does not limit the disclosed examples. Instead, the proper scope of the disclosed examples may be defined by the appended claims.

[0012] With the rapid growth in the use of electronic communication, data security has become more and more important. One way of providing data security is by data encryption. For example, original data may be encrypted through an encryption process using an encryption key. The encrypted data may be stored and transferred. To access the original data, the encrypted data may be decrypted by using a decryption key. The decryption key is synchronized with the encryption key.

[0013] However, in some current solutions, encrypted data may be copied so that multiple decryption attempts may be performed. In some cases, if enough attempts are made, the encrypted data may be forcedly decrypted.

[0014] Examples disclosed herein address these challenges by securing data with memristors. In an example method, a memristor is in one of a first resistance state and a second resistance state, representing binary data. An encryption is applied to the memristor to tune the memristor to a third resistance state. The encryption determines a decryption voltage that tunes the memristor from the third resistance state back to its original state. Applying the correct decryption voltage results in tuning the memristor back to the original state. Applying a wrong decryption key could result in non-tuning of the memristor or erroneous tuning, which results in permanent data loss.

[0015] Referring now to the drawings, FIG. 1A depicts a cross-sectional view of an example memristor in a first resistance state 100A, the memristor in a second resistance state 100B, and the memristor in a third resistance state 100C. Memristors 100A-100C may include a first electrode 110A, a second electrode 110B, and an active region 120 coupled between first electrode 110A and second electrode 110B.

[0016] Memristors 100A-100C may be electrical devices or components that provide switching and memory properties. Specifically, a memristor 100A-100C may change resistance when a voltage is applied across it or a current is driven through it. Furthermore, memristor 100A-100C may "memorize" its last resistance. In this manner, memristor 100A-100C may be set to at least two resistance states. When used as a basis for memory devices, memristors may be used to store a bit of information, such as a 1 or 0, represented by two resistance states. Memristor 100A-100C may be based on a variety of materials as described herein.

[0017] First electrode 110A and second electrode 110B may deliver voltage and/or current to active region 120 of memristor 100A-100C. First electrode 110A and second electrode 100B may be made of conducting materials, such as platinum (Pt), tantalum (Ta), hafnium (Hf), zirconium (Zr), aluminum (Al), cobalt (Co), nickel (Ni), iron (Fe), niobium (Nb), molybdenum (Mo), tungsten (W), copper (Cu), titanium (Ti), tantalum nitrides (TaN_x), titanium nitrides (TiN_x), WN_2, NbN, MoN, $TiSi_2$, TiSi, Ti_5Si_3, $TaSi_2$, WSi_2, $NbSi_2$, V_3Si, electrically doped Si polycrystalline, electrically doped Ge polycrystalline, and combinations thereof.

[0018] Active region 120 may be coupled between first electrode 110A and second electrode 110B. Active region 120 may include a plurality of ions 130. In some examples, the plurality of ions 130 may include oxygen anions. Active region 120 may be oxide-based, meaning that at least a portion of the active region is formed from an oxide-containing material, which may provide oxygen anions. In some examples, active region 120 may be formed based on tantalum oxide (TaO_x) or hafnium oxide (HfO_x) compositions. Other example materials of active region 120 may include titanium oxide, yttrium oxide, niobium oxide, zirconium oxide, aluminum oxide, calcium oxide, magnesium oxide, dysprosium oxide, lanthanum oxide, silicon dioxide, or other like oxides.

[0019] In some examples, active region 120 may also be nitride-based, meaning that at least a portion of the memristor is formed from a nitride-containing composition, such as aluminum nitride, gallium nitride, tantalum nitride, and silicon nitride. In such examples, the plurality of ions 130 may include nitrogen ions. Furthermore, memristors may be oxy-nitride based, meaning that a portion of the memristor is formed from an oxide-containing material

and that a portion of the memristor is formed from a nitride-containing material. In addition, other functioning materials may be employed in the practice of the teachings herein.

[0020] In some implementations, memristors may be coupled to other electrical components, such as selectors. Selectors may be electrical devices that may be used in memristor devices to provide desirable electrical properties. For example, selectors may be coupled in series with each memristor to increase the overall nonlinear characteristics of the memristors. Selectors may be based on a number of materials, including metal oxides and metal nitrides. Non-limiting examples include niobium oxide, tantalum oxide, vanadium oxide, titanium oxide, and chromium oxide.

[0021] Referring back to FIG. 1, the plurality of ions 130 may form a conducting filament 140 that is continuous through active region 120 in memristor 100A in the first resistance state. The conducting filament 140 may be formed by the alignment of ions 130. With the presence of conducting filament 140, memristor 100A may be relatively conducting, and in a relatively low resistance state.

[0022] The plurality of ions 130 may form conducting filament 140 with at least one disconnection 145 in active region 120 in memristor 100B in the second resistance state. In some examples, such as the one illustrated in FIG. 1, disconnection 145 may be formed towards an edge of active region 120. However, disconnection 145 may be formed at any point of conducting filament 140. With the disconnection 145 in conducting filament 140, memristor 100B may be relatively insulating, and in a first relatively high resistance state.

[0023] The memristor in the first resistance state 100A may be switched to the memristor in the second resistance state 100B by the application of a switching energy across the active region 120. The switching energy may be a current or a voltage, such as a writing voltage. Similarly, the memristor in the second resistance state 100B may be switched to the memristor in the first resistance state 100A by the application of a switching energy across the active region 120, such as an erasing voltage.

[0024] In some examples, a memristor may exhibit bipolar or unipolar switching. Bipolar memristors may depend on the polarity of an applied switching energy. Specifically, a bipolar memristor in the first resistance state 100A may be switched from the first state to the second

state by application of a voltage of a first polarity, while a bipolar memristor in the second resistance state 100B may be switched from the second state to the first state by application of a voltage of a second polarity. Unipolar memristors, on the other hand, may depend on the amplitude of an applied voltage or other factors.

[0025] In some examples, a memristor may have a third resistance state 100C in which plurality of ions 130 do not form a conducting filament such as conducting filament 140. In some examples, ions 130 may be dispersed in active region 120. In such conditions, the memristor may be relatively insulating, and in a second relatively high resistance state.

[0026] As described in detail herein, the memristor may be tuned to the third resistance state from the first resistance state or from the second resistance state by applying an encryption to the memristor. The encryption may be, for example any energy or stimulus that causes memristor tuning as described herein. For example, the encryption may be an energy that causes the dispersion of the plurality of ions 130. The encryption may be, for example, high photon energy, thermal energy, or mechanical energy.

[0027] The encryption may determine a decryption voltage which may tune the memristor from the third resistance state back to its original state. For example, the decryption voltage may be a voltage or range of voltages that causes the reformation of conducting filament 140. Further details of the decryption voltage is described below in reference to FIG. 3B.

[0028] Fig. 2 is a block diagram of an example system 200 for securing data with memristors. System 200 may include a plurality of memristors 210 and a security engine 220. The dotted line shows that the components of system 200 may be located together in a single device or that the components may be separate and functionally connected.

[0029] Plurality of memristors 210 may be utilized to store data, such as binary data. Plurality of memristors 210 may be arranged in a variety of orientations. In some examples, memristors 210 may be arranged in a crossbar array, where the memristors 210 may be coupled between row lines and column lines. Such an arrangement may facilitate density and efficiency as a data storage device. Each memristor may be in one of a low resistance state and a first high resistance state.

[0030] Analogous to the memristors described in relation to FIG. 1, each memristor may have an active region having a plurality of ions. The ions may form a conducting filament through the memristor which may determine the resistance state of the memristor. The conducting filament may be continuous through the memristor in the low resistance state. On the other hand, the conducting filament may have at least one disconnection in the memristor in the first high resistance state.

[0031] Security engine 220 may be a combination of hardware and programming to perform the functionality described herein. For example, security engine 220 may include processor-executable instructions stored on non-transitory machine-readable storage media. Security engine 220 may include a processor or other hardware to execute the processor-executable instructions.

[0032] For example, security engine 220 may have hardware, which may include driving circuitry and other electrical components, to apply an encryption to the plurality of memristors 210 to tune each memristor 210 to a second high resistance state. In some examples, the encryption may cause the disintegration of a conducting filament in the memristor. The encryption may an energy that causes the memristor tuning as described herein, such as high photon energy, thermal energy, or mechanical energy. In some examples, security engine 220 is to direct an electromagnetic radiation at the memristor to disperse ions forming the conducting filament.

[0033] In some examples, a memristor being tuned from the first high resistance state to the second high resistance state may retain the disconnection in the conducting filament. The memristor in the second high resistance state may not from a conducting filament through the memristor. In some examples, the plurality of ions may be dispersed in the active region of the memristor.

[0034] Furthermore, security engine 220 may have hardware to apply a decryption voltage to the plurality of memristors 210 to tune the memristors back to their original states. The decryption voltage may be determined by the encryption. For example, the amount of energy applied in the encryption may determine the voltage range which may form the conducting filament when tuning from the second high resistance state to the low resistance

state, but not form the conducting filament when tuning from the second high resistance state to the first high resistance state.

[0035] FIG. 3A illustrates a schematic cross-sectional view of an example memristor being tuned by an encryption. FIG. 3A is described herein in reference to system 200 of FIG. 2.

[0036] FIG. 3A illustrates a memristor in a low resistance state 300A, which may be analogous to the memristor in the first resistance state 100A of FIG. 1, and a memristor in a first high resistance state 300B, which may be analogous to the memristor in the second resistance state 100B of FIG. 1. Memristor 300A may have a continuous conducting filament through an active region, which may be coupled between electrodes. The conducting filament may be made up of a plurality of conducting ions. Memristor 300B may have a conducting filament of ions that may include a disconnection. Accordingly, memristor 300A may be more conducting, and therefore have a lower resistance, than memristor 300B.

[0037] An encryption 310 may be applied to memristor 300A and memristor 300B. For example, security engine 220 of system 200 may apply encryption 310 to cause the disintegration of a conducting filament in the memristors 300A and 300B. The encryption may be any energy that causes the memristor tuning as described herein, such as high photon energy, thermal energy, or mechanical energy. In some examples, security engine 220 is to direct an electromagnetic radiation at the memristors 300A-300B to disperse ions forming the conducting filament.

[0038] The application of encryption 310 may cause memristor in the low resistance state 300A to tune to a memristor in a second high resistance state 300C where the plurality of ions are dispersed within the active region. The application of encryption 310 may cause memristor in the first high resistance state 300B to tune to a memristor in a second high resistance state 300D where the plurality of ions are dispersed and where the disconnection in the conducting filament is retained in the active region. In some examples, the resistance of memristor 300C and 300D may be practically indistinguishable. In some other examples, the resistance of memristor 300C and memristor 300D may be slightly different due to the presence of the disconnection. Accordingly, memristor 300D may be considered to be in a third high resistance state.

[0039] In such a manner, data stored by the memristors may be secured. For example, memristor 300A may represent one of a 0 or a 1 in binary code. Memristor 300B may represent the other of a 0 or a 1 in binary code. After application of encryption 310, memristor 300C and memristor 300D are both in high resistance states due to the lack conducting filament. Therefore, memristor 300C and memristor 300D may be practically indistinguishable. Accordingly, the data may be encrypted for third parties.

[0040] FIG. 3B illustrates a schematic cross-sectional view of an example memristor being tuned by a decryption voltage. FIG. 3B is described herein reference to system 200 of FIG. 2.

[0041] FIG. 3B illustrates a memristor in a second high resistance state 350C, which may be analogous to memristor 300C of FIG. 3A, and a memristor in a second high resistance state 350D, which may be analogous to memristor 300D of FIG. 3A. Memristor 350C and memristor 350D may each have a plurality of ions dispersed within a respective active region. Memristor 350C and memristor 350D may represent encrypted data. For example, memristor 350C may have been tuned from a memristor in a low resistance state with a continuous conducting filament representing a 0 or 1 in binary code. Memristor 350D may have been tuned from a memristor in a first high resistance state with a disconnection in a conducting filament representing the other of 0 or 1 in binary code. However, after encryption, memristor 350C and memristor 350D may be electrically indistinguishable or they may not be able to be accurately matched with the state from which they were tuned.

[0042] To decrypt the data, a decryption voltage 360 may be applied to memristor 350C and memristor 350D. For example, security engine 220 of system 200 may apply decryption voltage 360 to cause the formation of a continuous conducting filament in memristor 350C to form memristor 350A in a low resistance state. Decryption voltage 360 may not cause the formation of a conducting filament in memristor 350D. Although not illustrated, alternatively, decryption 360 may cause the formation of a conducting filament in memristor 350D with the retained disconnection.

[0043] The voltage range in which the decryption voltage 360 may properly decrypt the data is determined by the encryption that had encrypted the data. For example, encryption 310 may determine how much voltage is need to restore the conducting filament in

memristor 350C and how much voltage is needed to restore the conducting filament in memristor 350D. The voltage range between these two voltages may be the proper range for decryption voltage 360 so that a continuous conducting filament is formed in memristor 350C but not in memristor 350D. A decryption voltage 360 outside of this range may not properly form a conducting filament in memristor 350C and/or improperly form a conducting filament in memristor 350D, thereby destroying the data stored in memristor 350D. In such a manner, encrypted data stored by the memristors may be decrypted by a correct decryption voltage.

[0044] FIG. 4A is a flowchart of an example method 400 for securing data with a memristor. Method 400 may include operation 410 for providing a memristor, and operation 420 for applying an encryption to tune the memristor. Although execution of method 400 is herein described in relation to the illustration in FIG. 3A, other suitable examples for implementation of method 400 should be apparent.

[0045] In an operation 410, a memristor may be provided where the memristor is in one of a first resistance state and a second resistance state. For example, the memristor may be analogous to a memristor in a low resistance state 300A where the memristor has a continuous conducting filament or to a memristor in a first high resistance state 300B where a conducting filament has a disconnection.

[0046] In an operation 420, an encryption may be applied to tune the memristor to a third resistance state. For example, encryption voltage 310 may be applied to tune a memristor in a low resistance state 300A to a second high resistance state like in memristor 300C and to tune a memristor in a first high resistance state 300B to a second high resistance state like in memristor 300D. For example, the encryption may disperse the ions in the memristor to disintegrate the conducting filaments. The encryption may determine a decryption voltage that tunes the memristor from the third resistance state back to its original state.

[0047] FIG. 4B a flowchart of an example method 430 for securing data with a memristor including decrypting secured data. In addition to operations 410 and 420, method 430 may include operation 440 for applying a decryption voltage to tune the memristor back to its original state. Although execution of method 430 is herein described in relation to the

illustrations in FIG. 3B, other suitable examples for implementation of method 430 should be apparent.

[0048] After execution of operations 410 and 420, a decryption voltage may be applied to the memristor to tune the memristor from the second high resistance state to its original state in an operation 440. For example, the memristor may be analogous to a memristor in a second high resistance state 350C or to a memristor in a second high resistance state 350D where a disconnection in a conductive filament is retained. The application of a decryption voltage 360 may tune memristor 350C to a memristor in a low resistance state 350A, whereas the decryption voltage may not tune memristor 350D or it may tune 350D to a memristor in a first high resistance state (not shown). In such a manner, encrypted data stored in the memristor may be decrypted by a correct decryption voltage.

[0049] FIG. 4C is flowchart of an example method 450 for securing data with a memristor including decrypting secured data including determining the original state of the memristor. Although execution of method 450 is herein described in relation to the illustrations in FIG. 3A and FIG. 3B, other suitable examples for implementation of method 450 should be apparent.

[0050] Operations 455, 460, and 465 may be analogous to operations 410, 420, and 440 of method 430, respectively. In an operation 470, the original state of the memristor may be determined. For example, a memristor in second high resistance state 350C or 350D may be tuned from a low resistance state 300A or a first high resistance state 300B, respectively. In many examples, there may not be an active operation for determining the original state of the memristor, but only resulting in a different response by the memristor to the application of the decryption voltage depending on its original state.

[0051] Responsive to determining that the original state of the memristor was a low resistance state, method 450 proceeds to an operation 475A. In operation 475A, the memristor tunes back to a low resistance state, as illustrated by the tuning of memristor 350C to memristor 350A in FIG. 3B.

[0052] Responsive to determining that the original state of the memristor was a first high resistance state, method 450 proceeds to an operation 475B. In operation 475B, the

memristor remains in the second high resistance state, as illustrated by the memristor 350D in FIG. 3B.

[0053] The foregoing describes a number of examples for securing data with memristors. It should be understood that the examples described herein may include additional components and that some of the components described herein may be removed or modified without departing from the scope of the examples or their applications. It should also be understood that the components depicted in the figures are not drawn to scale, and thus, the components may have different relative sizes with respect to each other than as shown in the figures.

[0054] It should be noted that, as used in this application and the appended claims, the singular forms “a,” “an,” and “the” include plural elements unless the context clearly dictates otherwise.

CLAIMS

What is claimed is:

1. A method for securing data, comprising:

providing a memristor, wherein the memristor is in one of a first resistance state and a second resistance state; and

applying an encryption to the memristor to tune the memristor to a third resistance state, wherein the encryption determines a decryption voltage that tunes the memristor from the third resistance state to its original state.

2. The method of claim 1, further comprising applying the decryption voltage to the memristor to tune the memristor from the third resistance state to its original state.

3. The method of claim 1, wherein the first resistance state is a low resistance state, the second resistance is a first high resistance state, and the third resistance state is a second high resistance state.

4. The method of claim 3, wherein the decryption voltage tunes the memristor from the third resistance state to the first resistance state, and wherein the decryption voltage does not tune the memristor from the third resistance state to the second resistance state.

5. The method of claim 3, wherein the memristor comprises a plurality of ions, wherein:

the plurality of ions is to form a conducting filament through the memristor;

the conducting filament is continuous through the memristor in the first resistance state;

the conducting filament has at least one disconnection in the memristor in the second resistance statement; and

the plurality of ions does not form the conducting filament through the memristor in the third resistance state.

6. The method of claim 5, wherein the memristor retains the disconnection in the third resistance state in response to being tuned from the second resistance state.

7. The method of claim 5, further comprising directing an electromagnetic radiation at the memristor to disperse ions of the plurality of ions forming the conducting filament.

8. A system for securing data, comprising:

a plurality of memristors, wherein each memristor is in one of a low resistance state state and a first high resistance state;

a security engine to apply an encryption to the plurality of memristors to tune each of the plurality of memristors to a second high resistance state, wherein the encryption determines a decryption voltage that tunes a memristor of the plurality of memristors from the second high resistance state to the low resistance state.

9. The system of claim 8, wherein the security engine is to apply the decryption voltage to the plurality of memristors to tune at least one memristor of the plurality of memristors from the second high resistance state to the low resistance state in response to the at least one memristor being tuned to the second high resistance state from the low resistance state.

10. The system of claim 8, wherein the memristor comprises a plurality of ions, wherein:

the plurality of ions is to form a conducting filament through the memristor;

the conducting filament is continuous through the memristor in the low resistance state;

the conducting filament has at least one disconnection in the memristor in the first high resistance statement, wherein the memristor retains the disconnection in the second high resistance state in response to being tuned from the first high resistance state; and

the plurality of ions does not form the conducting filament through the memristor in the second high resistance state.

11. The system of claim 10, wherein the security engine is to direct an electromagnetic radiation at the memristor to disperse ions of the plurality of ions forming the conducting filament.

12. A memristor for securing data, comprising:

a first electrode;

a second electrode;

an active region coupled between the first electrode and the second electrode, wherein the active region comprises a plurality of ions, wherein:

the plurality of ions forms a continuous conducting filament through the active region in a first resistance state;

the plurality of ions form a conducting filament with at least one disconnection in the active region in a second resistance state of the memristor; and

the plurality of ions do not form a conducting filament in a third resistance state of the memristor.

13. The memristor of claim 12, wherein the first resistance state is a low resistance state, the second resistance is a first high resistance state, and the third resistance state is a second high resistance state.

14. The memristor of claim 12, wherein applying an encryption to the memristor tunes the memristor from one of the first resistance state and the second resistance state to the third resistance state.

15. The memristor of claim 12, wherein applying a decryption voltage to the memristor tunes the memristor from the third resistance state to its original state.

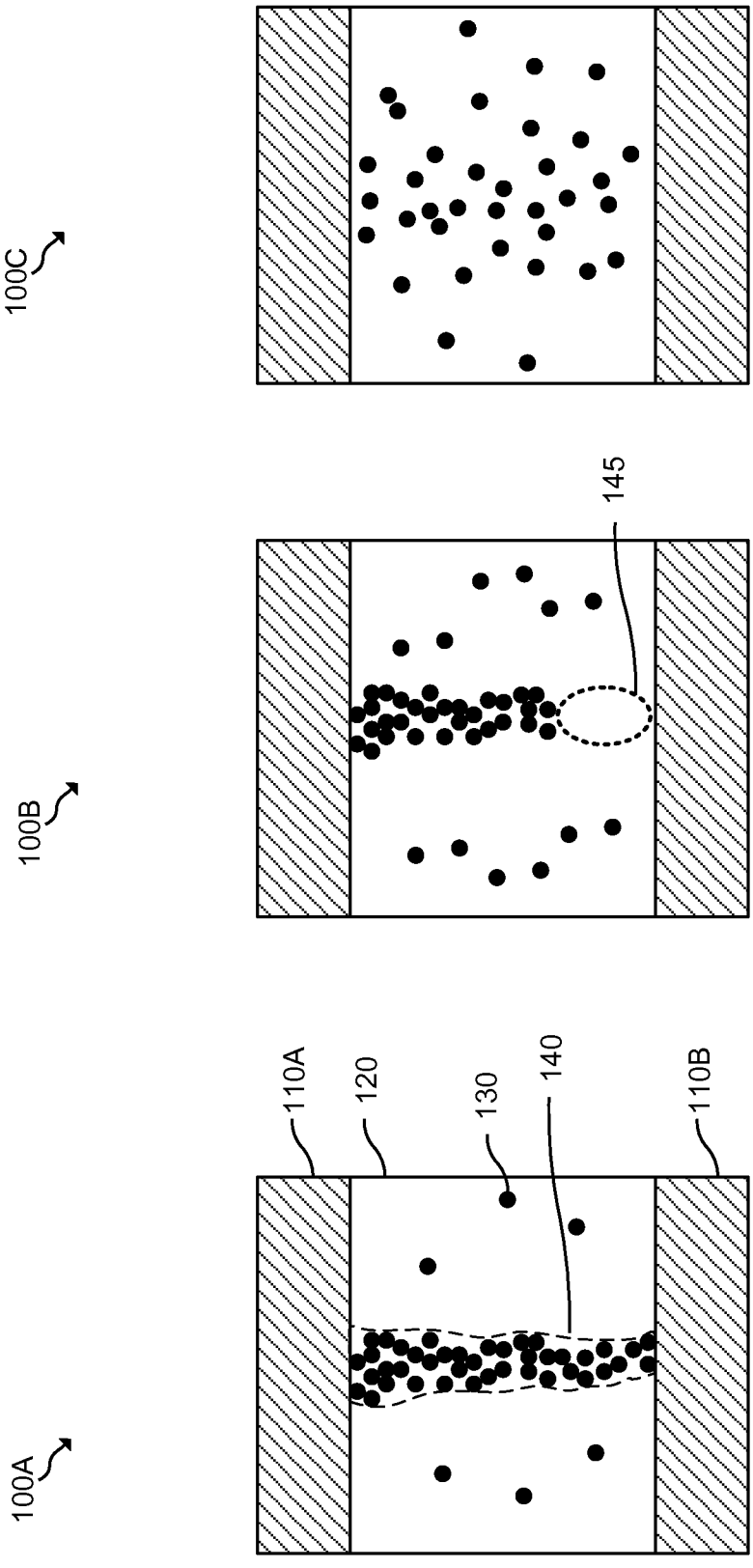

FIG. 1

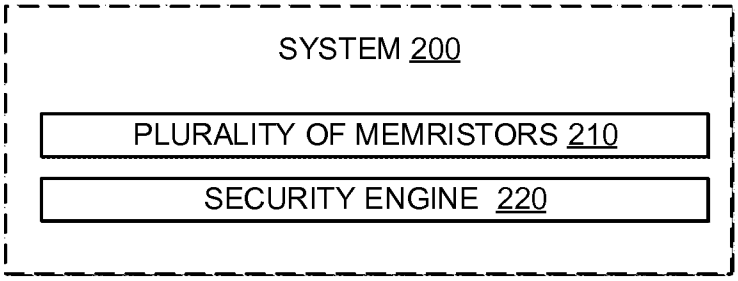
SYSTEM 200
PLURALITY OF MEMRISTORS 210
SECURITY ENGINE 220

FIG. 2

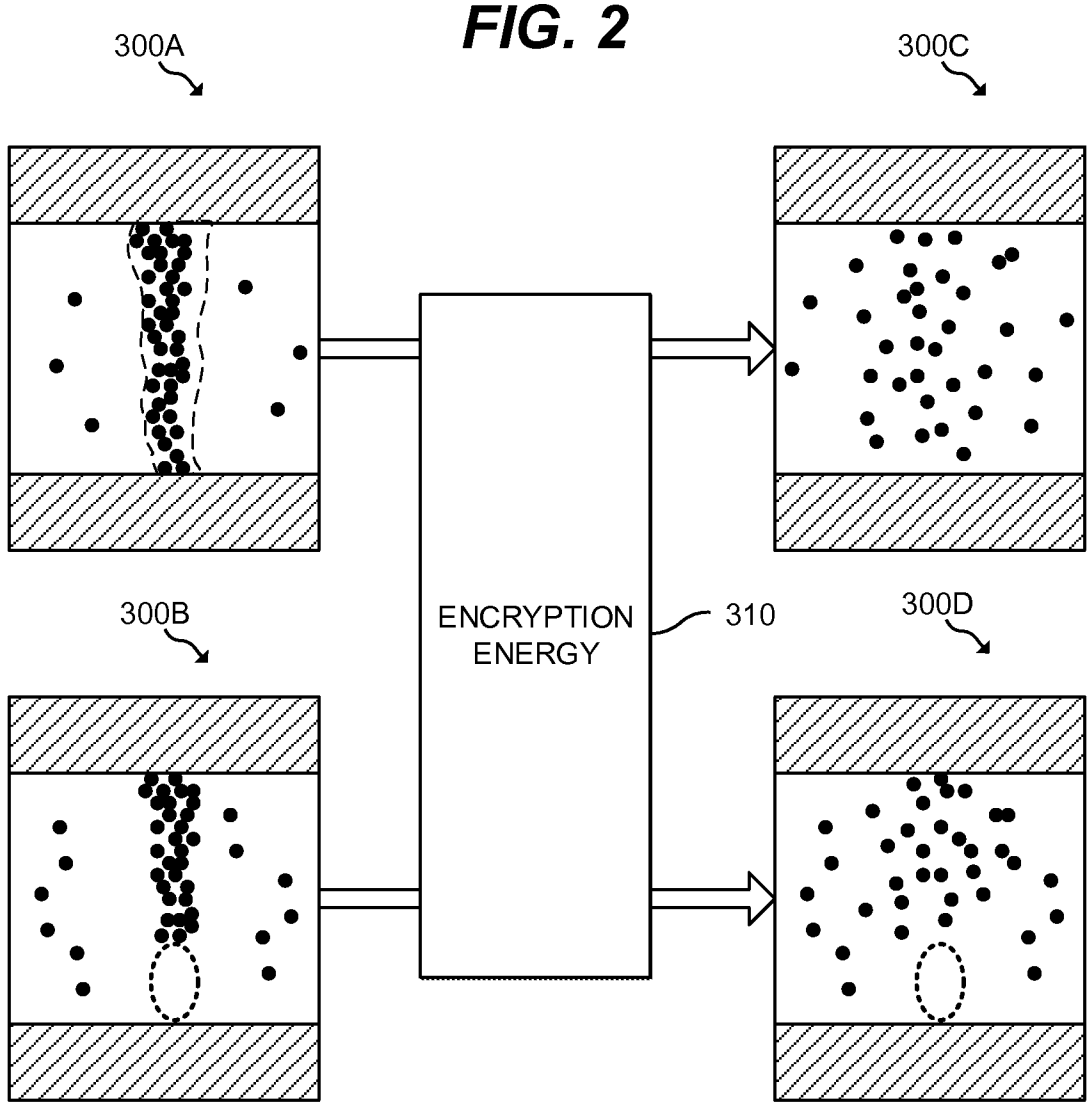
300A
300C
300B
300D
ENCRYPTION ENERGY
310

FIG. 3A

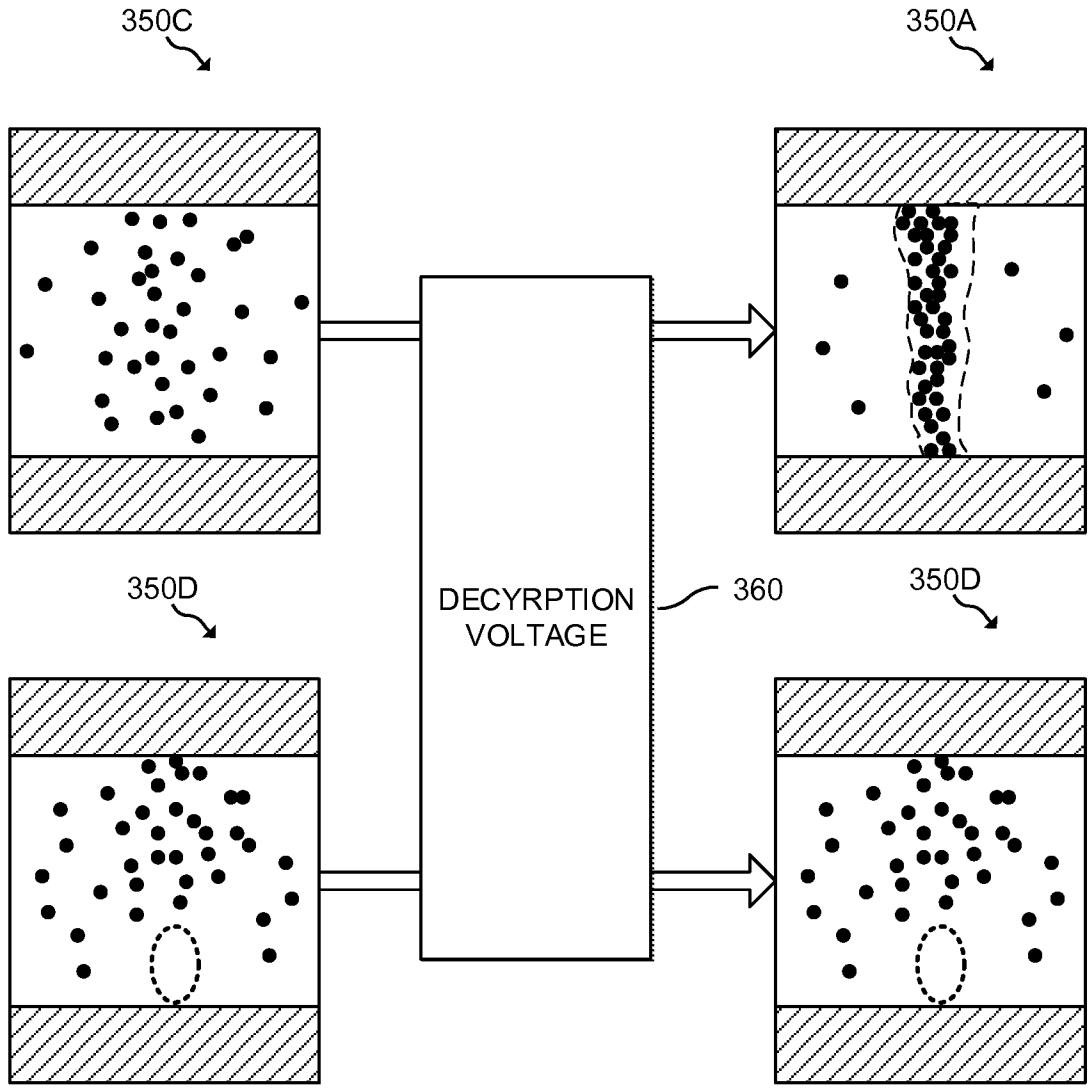

FIG. 3B

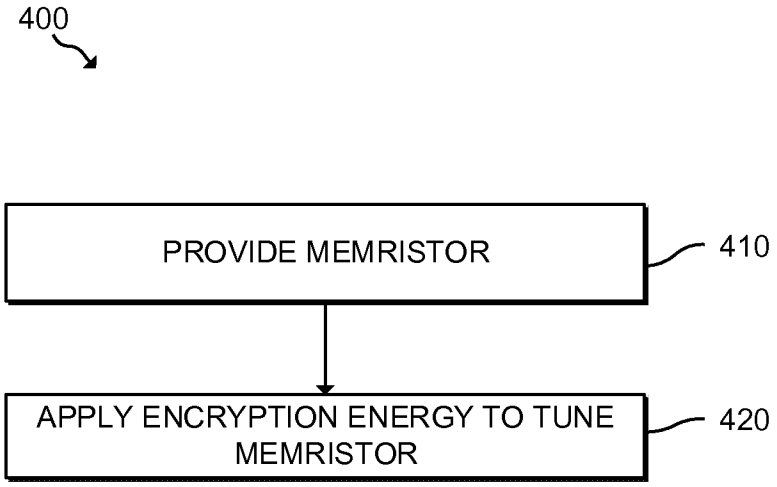
400
PROVIDE MEMRISTOR
410
APPLY ENCRYPTION ENERGY TO TUNE MEMRISTOR
420

FIG. 4A

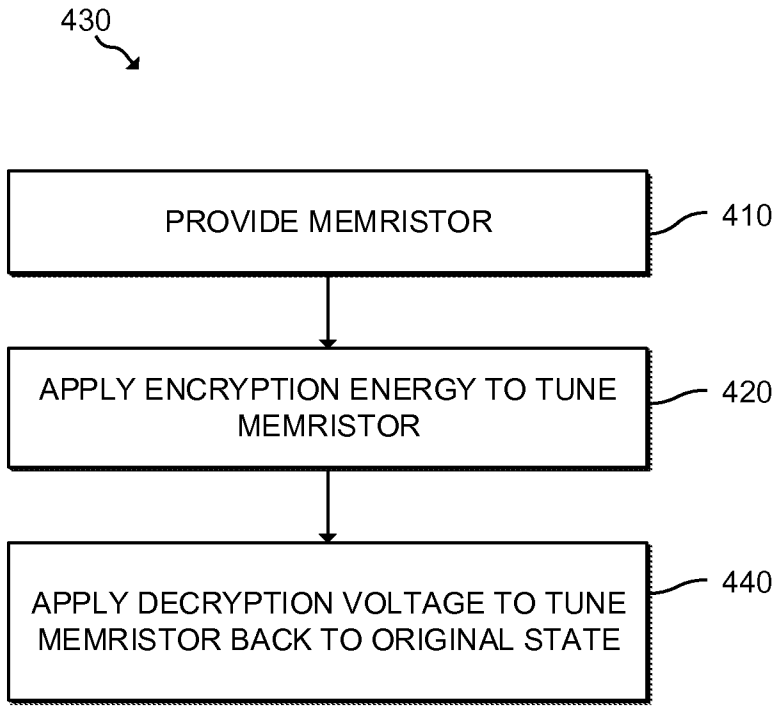
430
PROVIDE MEMRISTOR
410
APPLY ENCRYPTION ENERGY TO TUNE MEMRISTOR
420
APPLY DECRYPTION VOLTAGE TO TUNE MEMRISTOR BACK TO ORIGINAL STATE
440

FIG. 4B

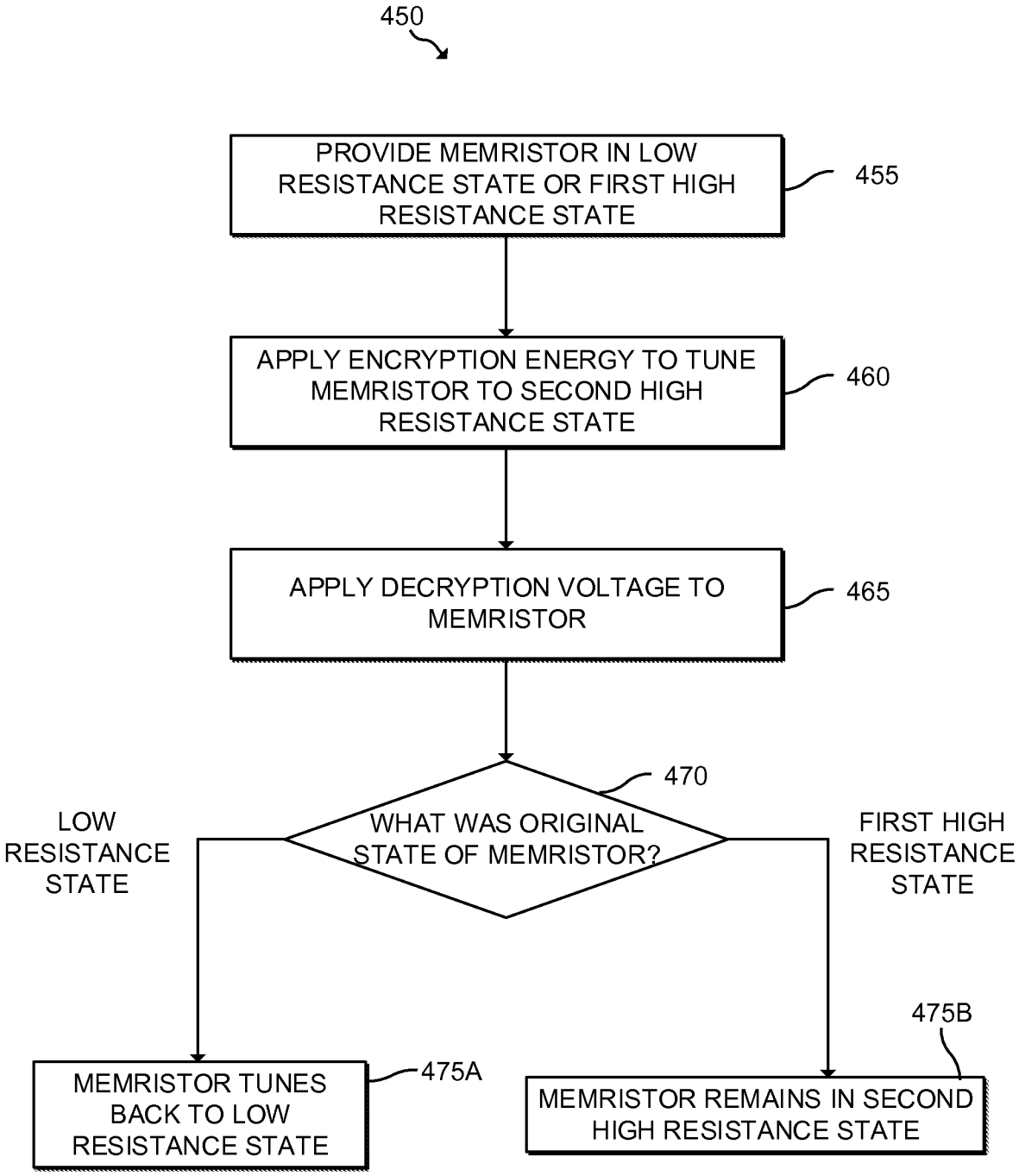
450
PROVIDE MEMRISTOR IN LOW RESISTANCE STATE OR FIRST HIGH RESISTANCE STATE
455
APPLY ENCRYPTION ENERGY TO TUNE MEMRISTOR TO SECOND HIGH RESISTANCE STATE
460
APPLY DECRYPTION VOLTAGE TO MEMRISTOR
465
470
WHAT WAS ORIGINAL STATE OF MEMRISTOR?
LOW RESISTANCE STATE
FIRST HIGH RESISTANCE STATE
MEMRISTOR TUNES BACK TO LOW RESISTANCE STATE
475A
475B
MEMRISTOR REMAINS IN SECOND HIGH RESISTANCE STATE

FIG. 4C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/049572

A. CLASSIFICATION OF SUBJECT MATTER

G11C 11/15(2006.01)i

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)
G11C 11/15; G11C 17/00; G06F 21/24; G06F 12/14; G06F 9/46; G06F 12/00; G11C 13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: memristor, resistance, third, state, encryption, decryption, voltage, tune, filament

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2013-0201748 A1 (SHINE C. CHUNG) 08 August 2013 See paragraphs [0004], [0035]-[0037]; and figures 1(a), 6(a)-6(b).	1-15
Y	US 2011-0302428 A1 (HANAN WEINGARTEN) 08 December 2011 See paragraphs [0025]-[0026]; and figures 4-5.	1-15
A	US 2014-0137119 A1 (RODERICK A. HYDE et al.) 15 May 2014 See paragraphs [0122]-[0132]; and figure 12A.	1-15
A	US 2014-0089683 A1 (ETHAN MILLER et al.) 27 March 2014 See paragraphs [0026]-[0043]; and figure 1.	1-15
A	US 2013-0054886 A1 (KAMRAN ESHRAGHIAN et al.) 28 February 2013 See paragraphs [0082]-[0085]; and figure 18.	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 application or patent 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
28 June 2016 (28.06.2016)	**29 June 2016 (29.06.2016)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
KIM, KI HO
Telephone No. +82-42-481-8691

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2015/049572

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013-0201748 A1	08/08/2013	US 9007804 B2	14/04/2015
US 2011-0302428 A1	08/12/2011	US 2011-246792 A1	06/10/2011
		US 8516274 B2	20/08/2013
		US 9104610 B2	11/08/2015
US 2014-0137119 A1	15/05/2014	None	
US 2014-0089683 A1	27/03/2014	CN 104704504 A	10/06/2015
		EP 2901357 A1	05/08/2015
		US 2014-250303 A1	04/09/2014
		US 8745415 B2	03/06/2014
		WO 2014-052420 A1	03/04/2014
US 2013-0054886 A1	28/02/2013	WO 2011-088526 A1	28/07/2011