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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
01 August 2019 (01.08.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/147246 A1

(51) International Patent Classification:
G06K 19/07 (2006.01) *G06K 7/10* (2006.01)
B65D 5/43 (2006.01)

(21) International Application Number:
PCT/US2018/015241

(22) International Filing Date:
25 January 2018 (25.01.2018)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.** [US/US]; 10300 Energy Drive, Spring, Texas 77389 (US).

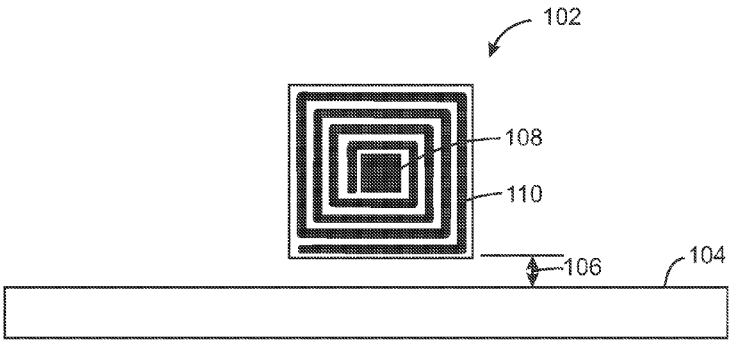
(72) Inventors: **IONESCU, Robert**; 1501 Page Mill Road, Palo Alto, California 94304 (US). **GE, Ning**; 1501 Page Mill Road, Palo Alto, California 94304 (US). **HOLDER, Helen A.**; 1501 Page Mill Road, Palo Alto, California 94304 (US). **WITTKOPF, Jarrid**; 1501 Page Mill Road, Palo Alto, California 94304 (US).

(74) Agent: **BURROWS, Sarah E.** et al.; HP Inc., 3390 East 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, JO, 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, 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,

(54) Title: SECURITY DEVICE FOR PRODUCT PACKAGING



100

FIG. 1

(57) Abstract: An RFID security device for product packaging is disclosed. The security device includes an RFID tag disposed on a first portion of a product package, and a booster antenna disposed on a second portion of the product package. The RFID tag and booster antenna are positioned on the product package so that the RFID tag will be electromagnetically coupled to the booster antenna when the product package is closed, and the RFID tag will be decoupled from the booster antenna when the product package is open.

WO 2019/147246 A1

[Continued on next page]

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))*

SECURITY DEVICE FOR PRODUCT PACKAGING

BACKGROUND

[0001] Radio Frequency Identification (RFID) tags are commonly used in various contexts such as product identification, inventory tracking, product security, and others. In a typical system, an RFID tag may be affixed to product packaging and encoded with product related information such as a product serial number, stock number, production date, and other identifying information. To read the tag, an RFID reader transmits a wireless signal to the RFID tag. In response to the wireless signal, the RFID tag wirelessly transmits its stored information to the RFID reader. The RFID reader is able to read the information from several RFID tags simultaneously, and may be configured to transmit responses to a computer system, which can use the information to track the product inventory.

DESCRIPTION OF THE DRAWINGS

[0002] Certain examples are described in the following detailed description and in reference to the drawings, in which:

[0003] Fig. 1 is a diagram of as security device disposed on a product package;

[0004] Fig. 2 is a diagram of another security device disposed on a product package;

[0005] Fig. 3 is a perspective view of an example package with a security device that includes an RFID tag and booster antenna;

[0006] Fig. 4 is a perspective view of another example package with a security device that includes an RFID tag and booster antenna;

[0007] Fig. 5 is a block diagram of an RFID security system; and

[0008] Fig. 6 is a block flow diagram summarizing a method 600 of manufacturing a product package with a security device.

DETAILED DESCRIPTION

[0009] Techniques for detecting package tampering are disclosed. The system includes an RFID tag and booster antenna disposed on the package. The booster antenna boosts the effective communication range of the RFID tag. The booster

antenna is disposed on one portion of the package, and the RFID tag is coupled to another portion of the package such that the RFID tag is inductively coupled to the booster antenna when the package is closed. When the package is opened, the RFID tag is decoupled from the booster antenna and the RFID reader loses communication with the RFID tag. This can be registered as a tampering event. When the package is opened, the RFID tag remains functional but has a reduced communication range. Resealing the package recouples the RFID tag and booster antenna so that normal operation of the RFID security system can resume.

[0010] Fig. 1 is a diagram of as security device disposed on a product package. The security device 100 includes an RFID tag 102 and booster antenna 104. Although not shown in Fig. 1, the RFID tag 102 and booster antenna 104 are disposed on different portions of a package that are movable relative to one another. The relative positions of the RFID tag 102 and booster antenna 104 shown in Fig. 1 occur when the package is closed such that the two portions of the package cause the RFID tag 102 and booster antenna 104 to be aligned. The alignment of the RFID tag 102 and booster antenna 104 cause the RFID tag 102 and booster antenna 104 to be electromagnetically coupled. As used herein, the term "electromagnetically coupled" refers to an inductive or capacitive coupling, as opposed to a conductive coupling. The edge-to-edge spacing 106 between the RFID tag 102 and the booster antenna 104 may be less than approximately 0.25 millimeters (mm) when the package is closed. In some examples, the RFID tag 102 and the booster antenna 104 may fully or partially overlap when the package is closed.

[0011] The RFID tag 102 includes an integrated circuit 108 and an antenna 110 conductively coupled to the integrated circuit 108 to enable the integrated circuit 108 to communicate wireless with an RFID reader. The RFID tag 102 may be active or passive. The integrated circuit 108 can include a non-volatile memory for storing various information, such as a unique tag serial number and product related information. The antenna 110 included in the RFID tag 102 enables the RFID tag 102 to communicate with the RFID reader over a short range of distances. For example, the communication range may be approximately 0 to 20 centimeters (cm) for the RFID tag 102 alone, i.e. without the booster antenna 104.

[0012] In some examples, the RFID tag 102, including the antenna 110 and integrated circuit 108, may be formed together as discrete unit and then coupled to the package using an adhesive. Other techniques are also possible. For example,

the antenna 110 of the RFID tag 102 may be printed onto the package and the integrated circuit 108 can be applied to the package over the antenna 110 and coupled to the package by an adhesive. The RFID tag 102 may also be coated with a sealing layer. In some examples, the RFID tag 102 may be embedded within the material of the package. For example, if the package is made of corrugated cardboard, the RFID tag 102 may be disposed between the layers of cardboard.

[0013] The booster antenna 104, when electromagnetically coupled to the RFID tag 102, increases the effective communication range of the RFID tag 102. For example, the booster antenna 104 may increase the communication range to a distance of around 10 centimeters to 2 meters. The booster antenna 104 may be any suitable type of antenna, including a monopole, dipole, meander dipole, loop antenna, and others. The booster antenna 104 may be disposed on the package in any suitable manner. In some examples, the booster antenna 104 may be made of a metal foil coupled to the package substrate by an adhesive. In some examples, the booster antenna 104 may be formed by printing a conductive medium on the package substrate using any of several printing techniques such as, thermal ink jet printing, liquid electrophotographic printing, and others.

[0014] Fig. 2 is a diagram of another security device disposed on a product package. As described in relation to Fig. 1, the RFID tag 102 and booster antenna 104 are disposed on different portions of package that are movable relative to one another. Fig. 2 shows the relative positions of the RFID tag 102 and booster antenna 104 when the package is in the closed position.

[0015] In the example shown in Fig. 2, the booster antenna 104 us a meander dipole. The bends in the booster antenna 104 reduce the footprint of the booster antenna 104 while maintaining a suitable resonant length. In this example, the booster antenna 104 also includes finger projections 200 to increase the coupling between the RFI tag and the booster antenna 104.

[0016] Fig. 3 is a perspective view of an example package with a security device that includes an RFID tag 102 and booster antenna 104. The example package shown in Fig. 3 is a box with an integrated lid 302 that folds over the top of the box. The body of the package 300 includes a tab 304 configured to mate with a slot 306 adjacent to the top surface of the lid 302. To fully close the package 300, the tab 304 is inserted into the slot 306. The open the package 300 without damaging it, the tab 304 must first be slid out from the slot 306.

[0017] As shown in Fig. 3, the RFID tag 102 may be disposed on a surface of tab 306, and the booster antenna 104 (shown with dotted lines) is disposed inside the box in the underside of the lid 302. When the tab 304 is inserted in the slot 306, the RFID tag 102 and booster antenna 104 will be in alignment as shown, for example, in Fig. 2. The alignment causes the RFID tag 102 to be electromagnetically coupled to the booster antenna 104, which increased the communication range of the RFID tag 102.

[0018] If the tab 304 is removed from the slot 306, the RFID tag 102 and booster antenna 104 become decoupled, which reduces the communication range of the RFID tag 102. The reduced communication range may cause an RFID reader to lose communication with the RFID tag 102. This loss of communication may indicate that the package 300 has been opened to access the package contents, and may be identified as a tampering event.

[0019] Although the RFID tag 102 may be unable to communicate with the RFID reader at long distances when the package 300 is in the opened state, the RFID tag 102 nevertheless remains operational. One advantage of the RFID tag 102 remaining operational is that the RFID tag 102 can still be used to identify and track the package 300. For example, an RFID reader may be brought to within a few centimeters of the RFID tag 102 to establish communicate with the RFID reader. Additionally, once the package 300 is reclosed, the RFID tag 102 becomes recoupled to the booster antenna 104 and is able to resume communications over the longer communication range. This may be useful, for example, if it can be confirmed that the product inside the package 300 is still present and unharmed.

[0020] The configuration shown in Fig. 3 is only one example configuration showing possible positions of the RFID tag 102 and booster antenna 104. It will be appreciated that other configurations are also possible. For example, the RFID tag 102 could be located on the bottom side of the tab 304 or embedded within the material of the tab 304. Similarly, the booster antenna 104 could be disposed on the top of the lid 302 or embedded within the material of the lid 302. The RFID tag 102 and booster antenna 104 may also be disposed on different portions of the package 300.

[0021] Fig. 4 is a perspective view of another example package with a security device that includes an RFID tag 102 and booster antenna 104. The example package shown in Fig. 4 is a box with an integrated lid 402 that folds over the top of

the box. The sides of the lid 402 include flaps 404 that are configured to slide into the body of the package 400 in contact with the inside surface of the side wall of the package 400.

[0022] As shown in Fig. 2, the RFID tag 102 may be disposed on a surface of one or the flaps 404, and the booster antenna 104 (shown with dotted lines) is disposed inside the body of the package 400 on the side wall 406 of the package 400. When the package 400 is closed, the flap 404 is inserted into the package 400 and the RFID tag 102 and booster antenna 104 will be in alignment as shown, for example, in Fig. 2. The alignment causes the RFID tag 102 to be electromagnetically coupled to the booster antenna 104, which increased the communication range of the RFID tag 102.

[0023] If the package 400 is opened, the RFID tag 102 and booster antenna 104 become decoupled, which reduces the communication range of the RFID tag 102. As described in relation to Fig. 3, the reduced communication range may cause an RFID reader to lose communication with the RFID tag 102, which indicates that the package has been opened and may be identified as a tampering event. As mentioned above, although the RFID tag 102 may be unable to communicate with the RFID reader at long distances when the package 400 is in the opened state, the RFID tag 102 nevertheless remains operational, and once the package 400 is reclosed, the RFID tag 102 becomes recoupled to the booster antenna 104 and is able to resume communications over the longer communication range.

[0024] The configuration shown in Fig. 4 is only one example configuration showing possible positions of the RFID tag 102 and booster antenna 104. It will be appreciated that other configurations are also possible. For example, the RFID tag 102 could be located on the bottom side of the inside facing side of the flap or embedded within the material of the flap. Similarly, the booster antenna 104 could be disposed on the outward facing side of the sidewall or embedded within the material of the sidewall. The RFID tag 102 and booster antenna 104 may also be disposed on different portions of the package. For example, the RFID tag 102 can be disposed on the forward facing flap, and the booster antenna 104 could be disposed on the forward facing sidewall. Additionally, multiple RFID tag 102 and booster antenna 104 pairs may be disposed on various corresponding portions of the lid and base.

[0025] Fig. 5 is a block diagram of an RFID security system. The system includes an RFID reader 502 in wireless communication with a number of RFID tags 102. Each of the RFID tags 102 is a component of a security device 100 coupled to a package 504. Each security device 100 includes the RFID tag 102 and the booster antenna 104 as described above. The RFID reader 502 can maintain continuous communication with each of the RFID tags 102 by periodically broadcasting an interrogation signal. Each RFID tag 102 may respond to the interrogation signal by transmitting its unique identification code and, in some implementations, additional product-related information.

[0026] In some examples, the RFID reader 502 is also in communication with a computer system 506, which may configured to collect and analyze data received from the RFID tags 102. The RFID reader 502 may be communicatively coupled to the RFID reader 502 through any suitable communication network, including wired connections, wireless connections, an Ethernet network, a WiFi network, the Internet, and others.

[0027] The computer system 506 may be configured to track inventory in any type of facility, such as a retail environment, and/or a storage facility such as warehouse, for example. The computer system 506 may also be coupled to additional RFID readers 502 within communication range of additional RFID tags 102 to provide coverage over a wider area.

[0028] In some examples, the computer system 506 is configured to detect product tampering. As described above, each of the RFID tags 102 will be within communication range of the RFID reader 502 while the package is closed. If any of the packages 504 is opened, the RFID tag 102 will be decoupled from its corresponding booster antenna 104, and the RFID reader 502 will stop receiving responses from the RFID tag 102. The resulting loss of communication can be flagged as a potential tampering event for the product associated with the RFID tag 102. This tampering event can be recorded by the computer system 506. In some examples, the computer system 506 may be configured to issue an alert to a staff member at the facility. If the package is reclosed, the RFID reader 502 may resume communication with the RFID tag 102. However, the tampering event will still be recorded, allowing a person to inspect the package to ensure product integrity.

[0029] Fig. 6 is a block flow diagram summarizing a method 600 of manufacturing a product package with a security device. At block 602 an RFID tag is disposed on a

first portion of a product package. The RFID tag may be fixed to a surface of the product package or embedded within the material of the product package. The RFID tag includes and RFID tag antenna and an RFID integrated circuit. In some examples, the RFID tag antenna may be printed on the product package and the RFID integrated circuit 108 may be coupled to the printed RFID antenna. In some examples, the RFID tag, including the RFID antenna and RFID integrated circuit, are created as a discrete unit and coupled to the package together.

[0030] At block 604, a booster antenna is disposed on a second portion of the product package. The booster antenna may be printed on a surface of the product package. In some examples, the booster antenna is manufactured separately and coupled to the product package. For example, the booster antenna may be made from a metal foil with an adhesive backing that can be attached to the product package. The RFID tag and booster antenna are positioned on the product package so that the RFID tag will be electromagnetically coupled to the booster antenna when the product package is closed, and the RFID tag will be decoupled from the booster antenna when the product package is open.

[0031] At block 606, product may be inserted into the product packaging and the product packaging may be closed so that the RFID tag is electromagnetically coupled to the booster antenna. Fewer or greater actions can be included in the method 600 depending on the design considerations of a particular implementation.

[0032] While the present techniques may be susceptible to various modifications and alternative forms, the examples discussed above have been shown only by way of example. It is to be understood that the techniques are not intended to be limited to the particular examples disclosed herein. Indeed, the present techniques include all alternatives, modifications, and equivalents falling within the scope of the present techniques.

CLAIMS

What is claimed is:

1. An RFID security apparatus for product packaging, comprising:
an RFID tag disposed on a first portion of a product package; and
a booster antenna disposed on a second portion of the product package;
wherein the RFID tag and booster antenna are positioned on the product package so that the RFID tag will be electromagnetically coupled to the booster antenna when the product package is closed, and the RFID tag will be decoupled from the booster antenna when the product package is open.

2. The RFID security apparatus of claim 1, wherein the booster antenna is printed on a surface of the product package.

3. The RFID security apparatus of claim 1, wherein the RFID tag is embedded within the material of the product package.

4. The RFID security apparatus of claim 1, wherein, when the product package is opened, the RFID tag remains operable with a reduced communication range compared to when the product package is closed.

5. The RFID security apparatus of claim 1, wherein the RFID tag is to communicate with an RFID reader while the product package is closed.

6. An RFID security system, comprising:
a product package comprising an RFID tag disposed on a first portion of the product package, and a booster antenna disposed on a second portion of the product package, wherein the RFID tag and booster antenna are positioned on the product package so that the RFID tag will be electromagnetically coupled to the booster antenna when the product package is closed, and the RFID tag will be decoupled from the booster antenna when the product package is open.
an RFID reader to communicate with the RFID tag while the product package is

closed.

7. The RFID security apparatus of claim 6, wherein the booster antenna is printed on a surface of the product package.

8. The RFID security apparatus of claim 6, wherein the RFID tag is embedded within the material of the product package.

9. The RFID security apparatus of claim 6, when the product package is opened, the RFID tag remains operable with a reduced communication range compared to when the product package is closed.

10. The RFID security apparatus of claim 6, wherein, when the product package is opened, the RFID reader loses communication with the RFID tag, and the RFID reader registers a tampering event in response to losing communication.

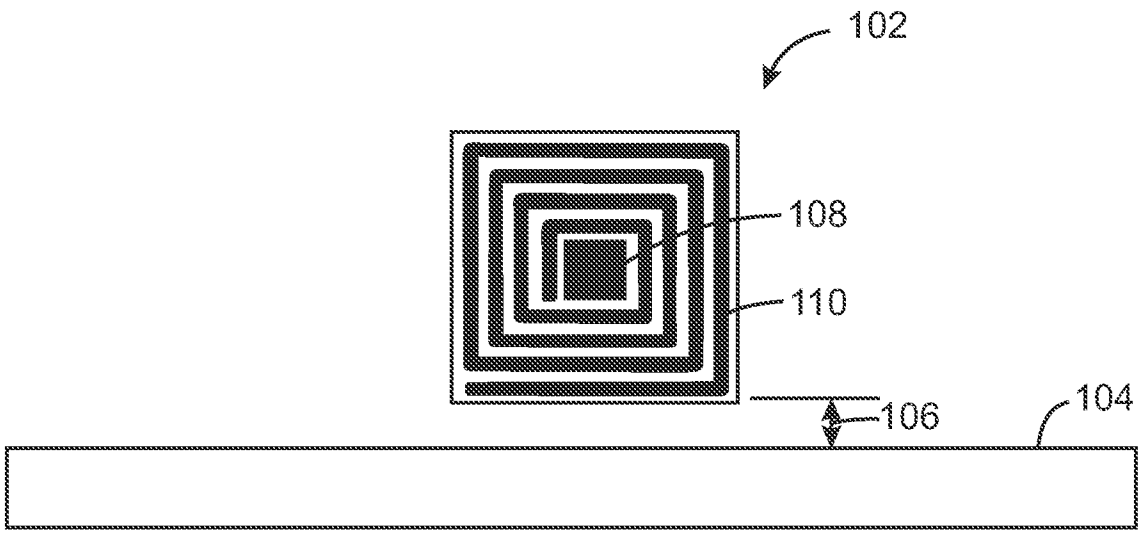
11. A method of manufacturing a product package with a security device, comprising:
disposing an RFID tag on a first portion of a product package;
disposing a booster antenna a second portion of the product package;
wherein the RFID tag and booster antenna are positioned on the product package so that the RFID tag will be electromagnetically coupled to the booster antenna when the product package is closed, and the RFID tag will be decoupled from the booster antenna when the product package is open.

12. The method of claim 11, wherein disposing the booster antenna on a first portion of a product package comprises printing the booster antenna on a surface of the product package.

13. The method of claim 11, wherein disposing an RFID tag on a first portion of a product package comprises embedding the RFID tag within the material of the product package.

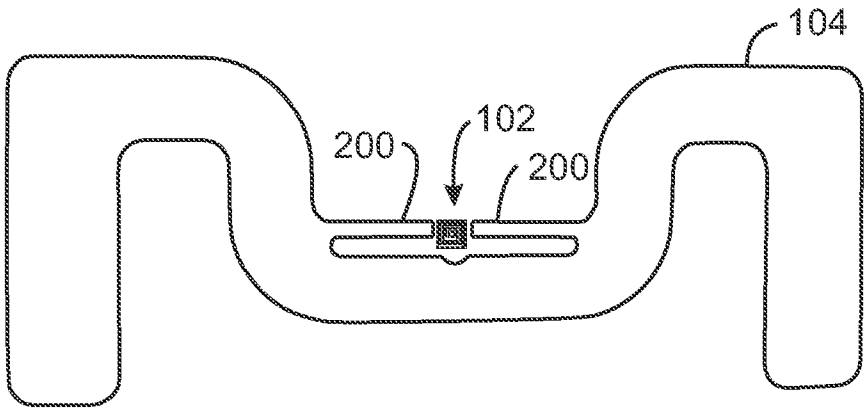
14. The method of claim 11, wherein, when the product package is opened, the RFID tag remains operable with a reduced communication range compared to when the product package is closed.

15. The method of claim 11, wherein the RFID tag is to communicate with an RFID reader while the product package is closed, and the RFID reader losses communication with the RFID tag when the product package is opened.



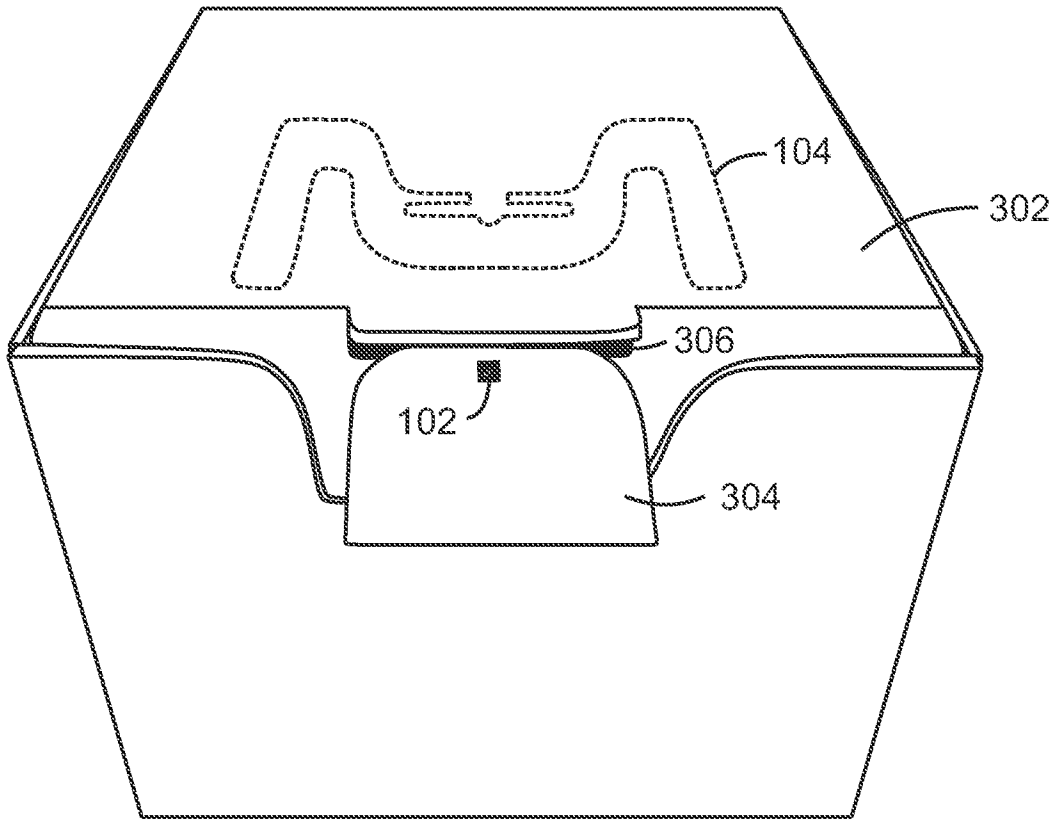
100

FIG. 1



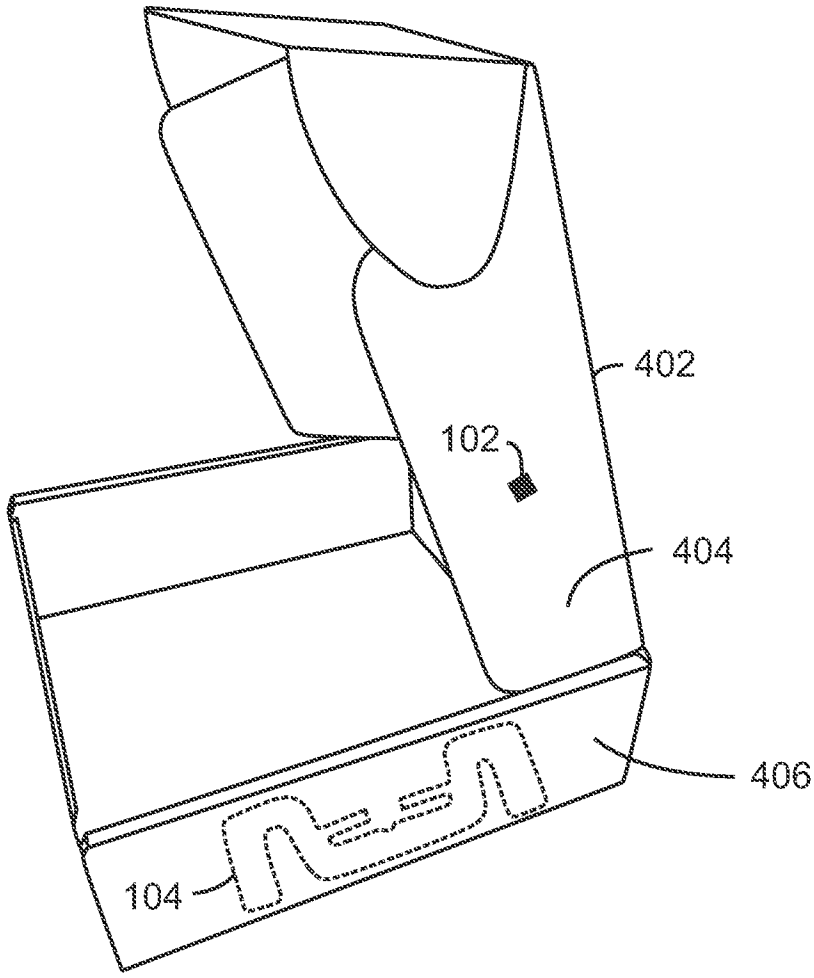
100

FIG. 2



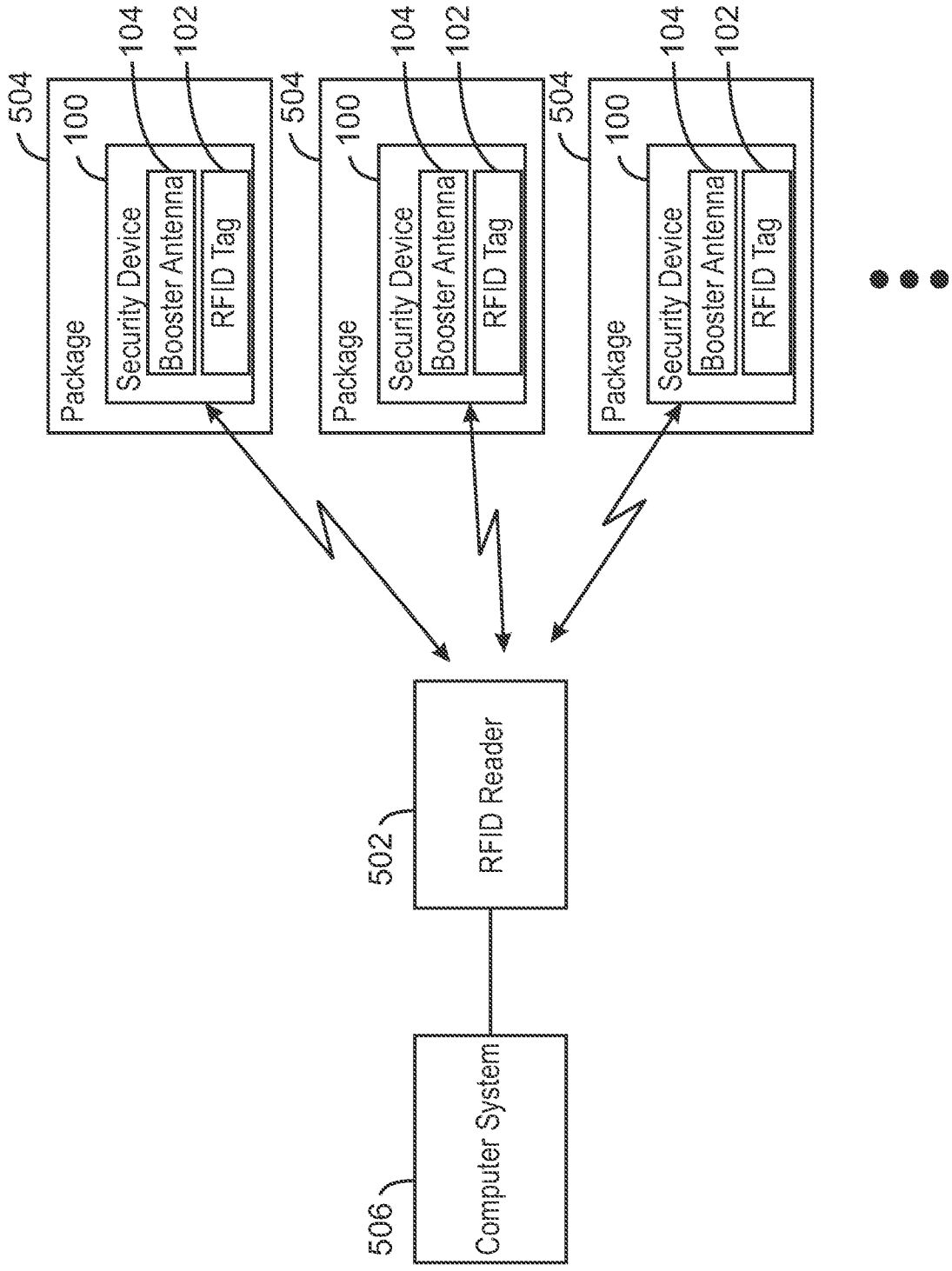
300

FIG. 3



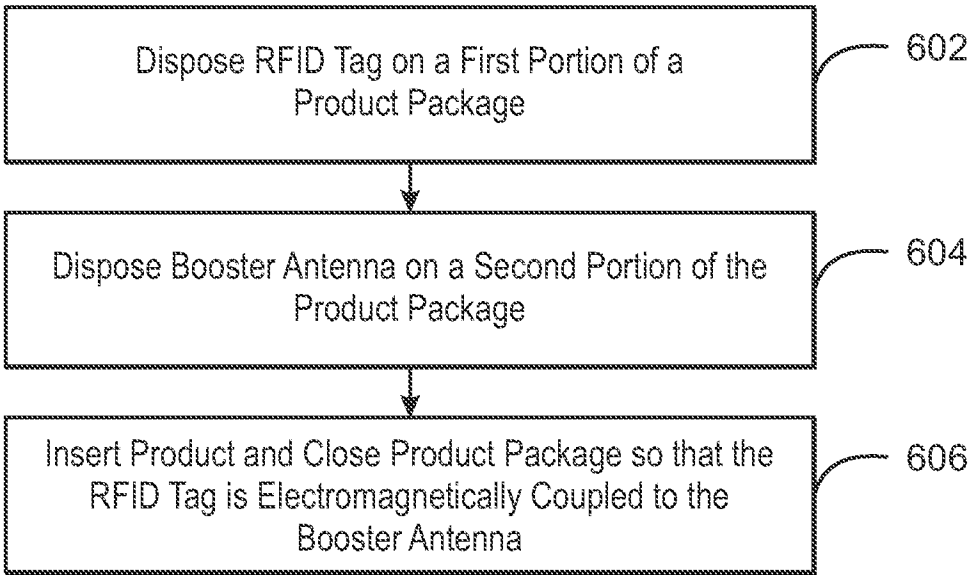
400

FIG. 4


504
100
104
102
Package
Security Device
Booster Antenna
RFID Tag
504
100
104
102
Package
Security Device
Booster Antenna
RFID Tag
504
100
104
102
Package
Security Device
Booster Antenna
RFID Tag
502
RFID Reader
506
Computer System

500

FIG. 5


Dispose RFID Tag on a First Portion of a Product Package
602
Dispose Booster Antenna on a Second Portion of the Product Package
604
Insert Product and Close Product Package so that the RFID Tag is Electromagnetically Coupled to the Booster Antenna
606

600

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 2018/015241

A. CLASSIFICATION OF SUBJECT MATTER

G06K 19/07 *(2006.01)*
B65D 5/43 *(2006.01)*
G06K 7/10 *(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)

B65D 5/00, 5/02, 5/42-5/66, 25/00-25/20, 79/00-79/02, G01N 27/00-27/02, G01R 31/00-31/02, G01V 15/00, G06K 7/00, 7/10, 9/00, 9/62, 19/00-19/077, G08B 13/00-13/14

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)

PatSearch (RUPTO internal), USPTO, PAJ, K-PION, Esp@cenet, Information Retrieval System of FIPS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2017/0363673 A1 (THIN FILM ELECTRONICS ASA) 21.12.2017, abstract, paragraphs [0002], [0006], [0046]-[0050], [0052], [0054]-[0055], [0058]-[0059], [0064], [0072], [0143]	1-15
A	US 2017/0364716 A1 (SMARTRAC INVESTMENT B.V.) 21.12.2017	1-15
A	US 2008/0068178 A1 (OWENS-ILLINOIS HEALTHCARE PACKAGING, INC.) 20.03.2008	1-15
A	US 2008/0309495 A1 (OWENS-ILLINOIS HEALTHCARE PACKAGING, INC.) 18.12.2008	1-15
A	US 5831531 A (MICRON COMMUNICATIONS, INC.) 03.11.1998	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
30 July 2018 (30.07.2018)	09 August 2018 (09.08.2018)
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 M. Demchenko Telephone No. (499) 240-25-91

Form PCT/ISA/210 (second sheet) (January 2015)