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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 February 2017 (02.02.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/015698 A1

(51) International Patent Classification:
H04B 5/02 (2006.01) *G06F 21/00* (2013.01)
G06K 19/00 (2006.01)

(21) International Application Number:
PCT/AU2016/050420

(22) International Filing Date:
27 May 2016 (27.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2015902950 24 July 2015 (24.07.2015) AU

(71) Applicant: **INFO WISE LIMITED** [CN/CN]; Room 1201, Allied Kajima Building, 138 Gloucester Road, Wanchai, Hong Kong (CN).

(72) Inventor; and
(71) Applicant *(for VC only)*: **YORKSTON, Simon** [AU/FR]; 29 Rue d'Alesia, Paris (FR).

(74) Agent: **CULLENS PATENT AND TRADE MARK ATTORNEYS**; Level 32, 239 George Street, Brisbane, 4000 (AU).

(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).

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

WO 2017/015698 A1

(54) Title: WIRELESS ACCESS TAG DUPLICATION SYSTEM AND METHOD

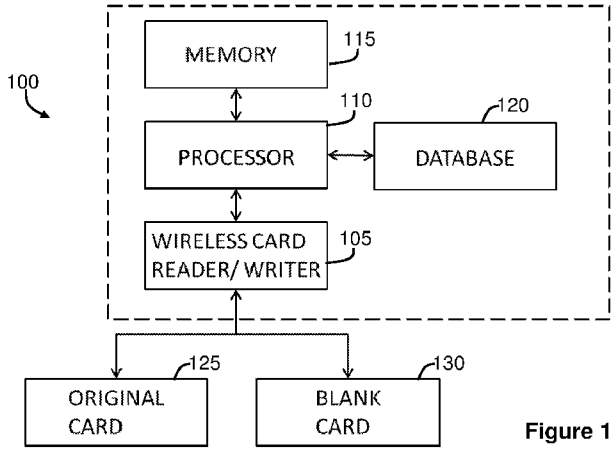

Figure 1

(57) Abstract: A wireless access tag duplication device, system and method is provided. The wireless access tag duplication system comprises: a wireless access tag reader; a wireless access tag writer; a processor, coupled to the wireless access card reader and the wireless access card writer; and a memory. The memory includes instruction code, executable by the processor, for: determining a first key of a first wireless access tag; determining remaining keys of the first wireless access tag using nested authentication and the first key; reading data of the first tag using the wireless access card reader, the first key and the remaining keys; and writing the data to a second tag using the wireless access card writer, the first key and the remaining keys.

WIRELESS ACCESS TAG DUPLICATION SYSTEM AND METHOD

TECHNICAL FIELD

[0001] The present invention relates to duplication of wireless access tags.

BACKGROUND ART

[0002] Traditionally, physical locks and keys were used to restrict access to buildings and other locations. In particular, a lock was typically placed on a door, which restricted access through the door unless a corresponding key was used.

[0003] Keys and locks were generally paired based upon a physical shape of the key. In particular, a barrel of the lock was configured to operate based upon the physical shape of the key. As such, a key could readily be copied by duplicating the shape of the key.

[0004] More recently, wireless access cards have gained popularity, as they enable more refined access control. For example, wireless access cards may be used to provide access to a building during business hours, but not after hours, and may also be used to log access to the building. Such refined access control is generally not possible with traditional keys alone.

[0005] However, a problem with wireless access cards is that they are difficult to copy. For example, Mifare wireless access cards are encrypted, which prevents the cards from being easily read or duplicated. As a result, instead of being able to copy access cards, cardholders are generally required to obtain additional unique cards which are programmed to provide the same access as the original card. This is generally costly, time consuming and inconvenient.

[0006] As a result, there is a need for an improved wireless access tag duplication system and method.

[0007] It will be clearly understood that, if a prior art publication is referred to herein, this reference does not constitute an admission that the publication forms part of the common general knowledge in the art in Australia or in any other country.

SUMMARY OF INVENTION

[0008] The present invention is directed to wireless access tag duplication systems and methods, which may at least partially overcome at least one of the abovementioned disadvantages or provide the consumer with a useful or commercial choice.

[0009] With the foregoing in view, the present invention in one form, resides broadly in a wireless access tag duplication system comprising:

a wireless access tag reader;

a wireless access tag writer;

a processor, coupled to the wireless access card reader and the wireless access card writer; and

a memory, including instruction code, executable by the processor, for:

determining a first key of a first wireless access tag;

determining remaining keys of the first wireless access tag using nested authentication and the first key;

reading data of the first tag using the wireless access card reader, the first key and the remaining keys and

writing the data to a second tag, using the wireless access card writer, the first key and the remaining keys.

[0010] Preferably, the first and second wireless access tags are wireless access cards. Suitably, the wireless access cards may be Mifare wireless access cards.

[0011] Preferably, the first and second wireless access tags include a plurality of data segments, wherein each data segment is associated with an encryption key.

[0012] Preferably, the first key is determined using a database of known keys. Suitably, each key in the database may be tested on the first wireless access tag. Alternatively, the first key may be determined using a brute force search.

[0013] The brute force search may comprise attempting to read data of the card to obtain a plurality of valid responses from the card; and exhaustively selecting a key that matches the valid responses.

[0014] The valid responses may be determined according to parity bits.

[0015] Alternatively, the brute force search may consider known characteristics of the tag to reduce the number of keys that are tested.

[0016] The system may be configured to attempt to determine the first key from the database, and perform a brute force only if the first key can not be determined from the database.

[0017] Preferably, the at least one remaining key is written to the database of known keys.

[0018] Preferably, the system is configured to determine a type of the first wireless access tag. The step of determining the first key of the first wireless access tag may be performed according to the type. The card type may generally determined by attempting to read data headers of the tag.

[0019] Preferably, the system is configured to determine a frequency of the first wireless access tag. Data may be read from the wireless access card at the determined frequency.

[0020] Preferably, determining the at least one remaining key comprises authenticating a first sector of the tag with the first key, and subsequently initiating authentication of a second sector of the tag to obtain a response from the tag, wherein a key of the at least one remaining keys is determined according to the response.

[0021] Preferably, the response comprises an encrypted challenge from the tag.

[0022] Preferably, a plurality of candidate keys are generated according to the encrypted challenge, and are verified against at least one other encrypted challenge to obtain the key of the at least one remaining key.

[0023] Preferably, determining the at least one remaining key further comprises subsequently initiating authentication of all remaining sectors of the tag to obtain responses from the tag, wherein keys of the at least one remaining key are determined according to the responses.

[0024] Preferably, the system includes a display. The display may be for displaying instructions to the user. The display may be for display a progress of tag duplication to the user.

[0025] The display may comprise a touch screen display, enabling the user to interact with the system. A graphical user interface may be displayed on the display, wherein the reading of the first card is initiated from the GUI.

[0026] The system may be configured to verify contents written to the second tag. In particular, the data of the second tag may be read, and the read data may be compared with the data of the first tag.

[0027] The second tag may include a mutable card identifier field, wherein an identifier from an immutable card identifier field of the first tag is written to the mutable card identifier field of the second tag.

[0028] The second tag may comprise a tag emulator. The tag emulator may include data corresponding to a plurality of first tags.

[0029] The system may include a data interface, for enabling communication with an external system. The communication may be performed via the Internet.

[0030] The system may be authenticated online. In particular, the system may require online authentication of an account prior to reading or writing to a tag.

[0031] Preferably, a unique identifier is associated with the system and an account. The unique identifier may be determined from hardware of the system. For example, the unique identifier may be determined in part according to a CPU IDof the system.

[0032] The system may include a single tag holder associated with both the wireless access tag reader and the wireless access tag writer. Alternatively, separate tag holders are associated with the wireless access tag reader and the wireless access tag writer.

[0033] Preferably, the system is configurable to write multiple copies of a tag without re-reading the original tag.

[0034] In another form, the present invention resides broadly in a wireless access tag duplication device comprising:

a wireless access tag reader;

a wireless access tag writer;

a processor, coupled to the wireless access card reader and the wireless access card writer; and

a memory, including instruction code, executable by the processor, for:

determining a first key of a first wireless access tag;

determining remaining keys of the first wireless access tag using nested authentication and the first key;

reading data of the first tag using the wireless access card reader, the first key and the remaining keys; and

writing the data to a second tag using the wireless access card writer, the first key and the remaining keys.

[0035] In yet another form, the present invention resides broadly in a wireless access tag duplication method comprising:

determining a first key of a first wireless access tag;

determining remaining keys of the first wireless access tag using nested authentication and the first key;

reading data of the first tag using a wireless access card reader, the first key and the remaining keys; and

writing the data to a second tag using a wireless access card writer, the first key and the remaining keys.

[0036] Any of the features described herein can be combined in any combination with any one or more of the other features described herein within the scope of the invention.

[0037] The reference to any prior art in this specification is not, and should not be taken as an acknowledgement or any form of suggestion that the prior art forms part of the common general knowledge.

BRIEF DESCRIPTION OF DRAWINGS

[0038] Various embodiments of the invention will be described with reference to the following drawings, in which:

[0039] Figure 1 illustrates a wireless access card duplication system, according to an embodiment of the present invention;

[0040] Figure 2a illustrates a perspective view of a wireless access card duplication device, according to an embodiment of the present invention;

[0041] Figure 2b illustrates a side view of the wireless access card duplication device of Figure 2a;

[0042] Figure 3 illustrates a wireless access card duplication method, according to an embodiment of the present invention; and

[0043] Figure 4 illustrates a method of determining encryption keys of a wireless access card, according to an embodiment of the present invention.

[0044] Preferred features, embodiments and variations of the invention may be discerned from the following Detailed Description which provides sufficient information for those skilled in the art to perform the invention. The Detailed Description is not to be regarded as limiting the scope of the preceding Summary of the Invention in any way.

DESCRIPTION OF EMBODIMENTS

[0045] Figure 1 illustrates a wireless access card duplication system 100, according to an embodiment of the present invention. The system 100 enables users, such as security consultants, locksmiths and/or residents, to easily and rapidly duplicate wireless access cards for keyless entry systems.

[0046] The system 100 includes a wireless card reader/writer 105, which is configured to read data from and write data to wireless access cards. Examples of such wireless access cards include the MIFARE family of cards (including the Mifare 1K, Mifare 4K, Mifare 8K, Mifare Ultralight, Mifare Ultralight C, Mifare Pro), the NTAG family of cards (including the NTAG210, NTAG212, NTAG213, NTAG215, NTAG216).

[0047] The card reader/writer 105 is coupled to a processor 110, which is in turn coupled to a memory 115 and a database 120. The memory 115 includes instruction code executable by the processor 110 for reading and writing cards, and the database 120 includes encryption keys, as discussed in further detail below.

[0048] In use, an original card 125 is read by the system 100. This includes determining encryption keys, and reading the original card 125 using the determined encryption keys.

[0049] A blank card 130 is then written with the data read from the original card 125.

[0050] As will be readily appreciated by the skilled addressee, the card reader/writer 105, the processor 110, the memory 115 and the database 120 may form part of a single device. In such case, the device may be portable, and thus used to duplicate cards on the fly.

[0051] Figure 2a illustrates a perspective view of a wireless access card duplication device 200, according to an embodiment of the present invention. Figure 2b illustrates a side view of the wireless access card duplication device 200. The wireless access card duplication device 200 may be similar or identical to the system 100 of Figure 1.

[0052] The device 200 comprises a housing 205, for housing a card reader/writer, such as the card reader/writer 105, a processor such as the processor 110, and a memory such as the memory 115. The housing 205 is formed of impact resistant plastic, to enable the device to be easily transported without damage.

[0053] The housing 205 defines a wireless access card holder 210, for receiving a wireless access card. The wireless access card holder 210 is located directly above the card reader/writer,

and is configured to retain a card adjacent to the card reader/writer.

[0054] The device 200 further includes a touchscreen display 215, for displaying data to a user, and receiving input from the user. As discussed in further detail below, a graphical user interface may be used to enable a user to interact with the system, including to initiating reading of a card, initiate writing of a card, to provide user credentials (such as a username and/or password), or interact with the device 200 in any other suitable way.

[0055] The device 200 further includes a local area network (LAN) port in the form of an RJ-45 Ethernet socket 220, and a pair of universal serial bus (USB) ports 225. The LAN port and the USB ports may be used to communicate with external systems, peripherals, or the like. For example, the LAN port may be coupled to a router providing Internet connectivity to the device 200. Similarly, the USB ports 225 may be used to couple a wireless modem, a keyboard, or any other suitable peripheral to the device 200.

[0056] In use, the user places the card to be copied on the wireless access card holder 210, and initiates reading of the card data using the touchscreen display 215. In particular, a graphical user interface (GUI) is displayed, which includes a "start scanning" virtual button. In short, the GUI guides the user through the card duplication process,

[0057] Upon selection of the start scanning button, the data of the card is read, as discussed in further detail below, and a progress bar is presented to the user on the touchscreen display 215. The progress bar provides instant feedback to the user that the card is being scanned, which helps prevent the card from being removed from the wireless access card holder 210 prematurely.

[0058] Upon completion of the reading of the data from the card, an indication that the reading is complete, and that the user may remove the card, is displayed on the touchscreen display 215. The graphical user interface then instructs the user to place a blank card on the wireless access card holder 210, and after which writing of the data to the blank card is initiated.

[0059] A progress bar is presented to the user on the touchscreen display 215, and upon completion of writing to the card, a message is displayed to the user indicating same. As such, the user is made aware of the progress of the writing of the card, as it is happening, which alleviates the problem of the user prematurely removing the card from the wireless access card holder 210, and thus preventing the writing of the card to complete.

[0060] As discussed in further detail below, the device 200 may attempt to verify data

written to the card. According to certain embodiments, the device 200 automatically reads the written card upon completion, and compares the written data to the data on record, to verify that all data has been written to the card correctly.

[0061] According to other embodiments (not illustrated), the device 200 includes first and second wireless access card holders, the first for the card being copied and second for the blank card. This enables completely unattended duplication as the device is able to read the card being copied and automatically write the data therefrom to the blank card.

[0062] The device 200 is compact and portable. As such, the device may be transported and used where required, including on-site, in portable offices, or the like. Alternatively, the device may be attached to a counter, a desk or the like, to prevent unwanted movement.

[0063] Figure 3 illustrates a wireless access card duplication method 300, according to an embodiment of the present invention. The card duplication method 300 may be incorporated into the system 100 of Figure 1 and/or the device 200 of figure 2 to provide card duplication functionality.

[0064] At step 305, a frequency of the card is determined. Typically, access cards operate at either 125kHz or 13.56 MHz, and as such, these frequencies are generally tested.

[0065] At step 310, a type of the card is determined. Examples of card types include the Mifare 1K card, as discussed above. The card type is generally determined by attempting to read headers of the card using the frequency determined earlier and known data protocols.

[0066] If the card is an encrypted card type, encryptions keys of the card are determined at step 315. In particular, keys used to encrypt data on the card are determined in this step, which enables retrieval of the data of the card. Figure 4, below, provides further details of a method to determine encryption keys of the card that may be used together with the method 300.

[0067] At step 320, the data of the card is read. As will be readily appreciated by the skilled addressee, if the card type is a non-encrypted card type, the method may proceed directly from step 310 to 320, without determining any encryption keys, as this is not required to read the data.

[0068] The card may comprise a plurality of data segments, and each data segment may be read individually. Each data segment may also be associated with a different encryption key. In the case of the Mifare Classic wireless access card, for example, the memory is divided into sectors, each of the sectors having 64 bytes and having its own 48-bit encryption key.

[0069] At step 325, the data from step 320 is written to the card. In case the card is encrypted, the data may be written to the card using the encryption key identified in step 315. The new card may then be used in place of the original card.

[0070] According to certain embodiments, the data from the original card includes an identifier field, which contains an identifier that is unique to the card and immutable. In such case, the new card may includes a mutable identifier field, which enables the identifier of the original card to be written thereto, allowing for perfect duplicates of the original card to be made.

[0071] According to certain embodiments, the data of the new card is read, and the read data of the new card is compared with the read data of the old card. If any discrepancies are found, a message may be displayed to the user. In some embodiments, the card may be automatically cleared and rewritten.

[0072] Figure 4 illustrates a method 400 of determining encryption keys of a wireless access card, according to an embodiment of the present invention. As discussed above, the method 400 may be used to determine the encryption keys in step 315 of the method 300.

[0073] The memory of the Mifare Classic wireless access card, for example, is divided into sectors, each of the sectors having its own 48-bit encryption key. To read data from a specific sector, the reader must first authenticate with the sector using the encryption key associated with that sector. As such, to be able to read the entire wireless access card, all encryption keys must be known.

[0074] At step 405, it is determined if one of the encryption keys of the card is in a database of keys. In particular, the database is stored and maintained for known keys of wireless access cards, and as a new key is determined, it is added to the database.

[0075] If no known key is used on the wireless access card, a key of the access card is determined using a brute force search.

[0076] In particular, read attempts are made to a sector using random data as the key and parity bits. When the parity bits are correct, which is a 1/256 chance for 8 parity bits, the wireless access card responds with an encrypted 4-bit error code. By repeating the process, sufficient data can be obtained to enable a brute force attack, and each key combination can be tested to determine which produces the correct parity bits and received response for the above obtained data.

[0077] The skilled addressee will readily appreciate that the brute force attack need not consider each key combination, but may instead utilise known characteristic of the card to reduce the number of keys considered, and thus increase a speed of the method.

[0078] As an illustrative example, predictions may be made in relation to the certain bits of a bitstream, if it is found that some bits do not depend on other bits of the bitsteam, which can reduce the number of keys required to be tested. Similarly, small levels of variability in the generation of the bitstream may also be exploited to reduce the number of keys required to be tested.

[0079] As a brute force attack is processor intensive, it is desirable to avoid this step. As the collection of pre-known keys gets larger, the chance of being able to avoid a brute force search is reduced.

[0080] At step 410, the remaining keys are determined using nested authentication and either the pre-known or the key determined in step 410.

[0081] In the case of Mifare Classic wireless access card, mentioned above, a known encryption key of one sector can be used to obtain information about the encryption key of another sector. In particular, a known encryption key may be used to authenticate the sector with which it is associated, and subsequent attempts to authenticate another sector provide about 32 bits of information about the secret key of that sector. This is due to the fact that the random number generator has only a 16-bit state, because parity bits of the card leak information, and because the tag's random number generator runs in sync with the communication timing.

[0082] Once the known encryption key us used to authenticate the first sector, the subsequent attempt to authenticate the second sector results in a challenge of the tag being sent encrypted. Then, a plurality of candidate keys, in this case 2^{16} (just over 65,000) candidate keys, are generated based upon the challenge and are checked using a second and possibly third authentication attempt. All candidate keys can generally be tested in under a second using ordinary hardware.

[0083] In most cases, a candidate key can be determined based upon two authentication attempts, however in some cases a third authentication attempt may be required if the intersection of the first and second attempts results in more than one key.

[0084] The above process is then repeated for all remaining sectors of the card.

[0085] While step 405 is illustrated prior to step 410 in the process flow, the skilled addressee will readily appreciate that step 410 may be performed in parallel to step 405. In such case, no delay is occurred by waiting for step 405 to be completed prior to initiating step 410.

[0086] An example of determining keys of a Mifare Classic wireless access card is outlined in Flavio D. Garcia, Peter Rossum, Roel Verdult, and Ronny Wichers Schreur "Wirelessly Pickpocketing a Mifare Classic Card", IEEE Symposium on Security and Privacy, IEEE, 2009, which is incorporated herein by reference.

[0087] According to certain embodiments, known keys are grouped in the database by statistical relevance, to reduce the time of the key testing process. Improvements in the keay searching can be achieved due to the fact that generally, each company that produces badges uses their own combination of keys.

[0088] According to certain embodiments, the system is coupled to an online payment system. In such case, a subscription may be employed where each copy made incurs a cost, and/or where use of the system is paid per day, week, month or similar. As an illustrative example, a user may be required to pay a monthly subscription fee as well as an individual card copying fee per card that is copied by the system.

[0089] According to certain embodiments, the wireless access card duplication device includes a unique identifier that is associated with an account. The unique identifier may be determined from a central processing unit (CPU) identifier (ID) associated with the device, or by any other suitable means. As such, the wireless access card duplication device may identify itself online without necessarily requiring user details. Alternatively, a username and password may be employed as authentication means.

[0090] The system may require internet access to enable the device to boot, or to enable the device to be able to write a card. This is particularly advantageous when subscription models may change over time, as the user may be forced to update the system to continue using baseline functionality of the device.

[0091] Such subscription models may be used to subsidise the cost of the wireless access card duplication device.

[0092] According to certain embodiments, each new card is associated with a unique identifier, to prevent the use of counterfeit cards. Validation is performed on new cards prior to data being written to the new card, and data is only written upon successful validation.

[0093] In particular, a database of valid cards, and their associated identifiers, is maintained centrally, and the respective identifier is stored on each valid card. When a user attempts to use a new card with the system, the identifier is read from the card, and compared with the valid identifiers in the database to ensure that the badge is genuine. If the identifier is genuine, it is then removed from the database (or marked as "used"), so that it cannot be used to subsequently verify other cards, to prevent the copying of multiple badges with a single identifier.

[0094] In other embodiments, the blank cards are rewritable. In such case, to prevent fraudulent blank cards from being used with the system, while enabling legitimate cards to be written to multiple times, each time a card is written, a fingerprint (or hash) is generated based upon the card data and the card identifier, which is saved in the database. The fingerprint is then later used to verify that the same card is being rewritten.

[0095] Alternatively, offline variations of the system may be provided, where a one-off fee is provided to utilise the technology indefinitely. This is particularly advantageous where large numbers of cards are being copied, or where internet access may not be available.

[0096] According to certain embodiments, the system may be configured to provide multiple copies of the same card, without requiring that the card be read multiple times. In such case, the data of the card is stored in memory and written as many times as required.

[0097] According to certain embodiments, the system enables remote administration, for example to provide maintenance or support. In particular, each device can be accessed remotely, via a reverse secure shell (SSH) tunnel, allowing a technician to remotely control the device to perform maintenance or provide support.

[0098] Similarly, software updates may be provided automatically or manually over the Internet, or by a software update on a USB key. The updates can add functionality to the device, improve performance, correct bugs, and allow for a full system recovery in case of software failure.

[0099] The system may be at least partly cloud based. For example, data may be sent to a remote server to determine key data, and the keys may be returned to the device for decoding. This is particularly advantageous for processor intensive activities such as brute force attacks.

[00100] The term "card" is primarily used in the specification above. However, wireless tags need not have the form of a traditional card, but can instead be any suitable shape. As an illustrative example, a wireless tag may be key-fob shaped.

[00101] In the present specification and claims (if any), the word 'comprising' and its derivatives including 'comprises' and 'comprise' include each of the stated integers but does not exclude the inclusion of one or more further integers.

[00102] Reference throughout this specification to 'one embodiment' or 'an embodiment' means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearance of the phrases 'in one embodiment' or 'in an embodiment' in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more combinations.

[00103] In compliance with the statute, the invention has been described in language more or less specific to structural or methodical features. It is to be understood that the invention is not limited to specific features shown or described since the means herein described comprises preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims (if any) appropriately interpreted by those skilled in the art.

CLAIMS

1. A wireless access tag duplication system comprising:

a wireless access tag reader;

a wireless access tag writer;

a processor, coupled to the wireless access card reader and the wireless access card writer; and

a memory, including instruction code, executable by the processor, for:

determining a first key of a first wireless access tag;

determining remaining keys of the first wireless access tag using nested authentication and the first key;

reading data of the first tag using the wireless access card reader, the first key and the remaining keys; and

writing the data to a second tag using the wireless access card writer, the first key and the remaining keys.

2. The system of claim 1, wherein the first and second wireless access tags comprise wireless access cards.

3. The system of claim 2, wherein the wireless access cards comprise Mifare wireless access cards.

4. The system of claim 1, wherein the first and second wireless access tags include a plurality of data segments, wherein each data segment is associated with an encryption key.

5. The system of claim 4, wherein a first key of the first wireless access tag is determined using a database of known keys.

6. The system of claim 4, wherein a first key of the wireless access tag is determined using a brute force search on the first wireless access tag.

7. The system of claim 6, wherein the brute force search comprises attempting to read data of the first wireless access tag to obtain a plurality of valid responses from the card; and

exhaustively selecting a key that matches the valid responses.

8. The system of claim 7, wherein the valid responses are determined according to parity bits.

9. The system of any one of claims 6 to 8, wherein the brute force search is performed according to known characteristics of the first wireless access tag to reduce the number of keys that are tested.

10. The system of any one of claims 6 to 9, configured to attempt to determine the first key from a database of known keys, and perform the brute force search in response to determining that the first key is not in the database.

11. The system of claim 10, wherein the remaining keys are written to the database of known keys.

12. The system of claim 1, configured to determine a type of the first wireless access tag, and determine the first key of the first wireless access tag according to the type.

13. The system of claim 1, configured to determine a frequency of the first wireless access tag, and read data from the wireless access card at the determined frequency.

14. The system of claim 1, wherein determining the remaining keys comprises authenticating a first sector of the tag with the first key, and subsequently initiating authentication of a second sector of the tag to obtain a response from the tag, wherein a key of the remaining keys is determined according to the response.

15. The system of claim 14, wherein the response comprises an encrypted challenge from the tag.

16. The system of claim 15, wherein a plurality of candidate keys are generated according to the encrypted challenge, and are verified against at least one other encrypted challenge to obtain the key of the at least one remaining key.

17. The system of claim 16, wherein determining the remaining keys comprises initiating authentication of all remaining sectors of the tag to obtain responses from the tag, wherein keys of the remaining keys are determined according to the responses.

18. The system of claim 1, further comprising a display, for displaying instructions to the user.

19. The system of claim 18, wherein the display is further configured to display a progress of tag duplication to the user.

20. The system of claim 18, wherein the display comprises a touch screen display, enabling the user to interact with the system.

21. The system of claim 1, further configured to verify contents written to the second tag.

22. The system of claim 1, wherein the second tag includes a mutable card identifier field, and wherein an identifier from an immutable card identifier field of the first tag is written to the mutable card identifier field of the second tag.

23. The system of claim 1, wherein the second tag comprises a tag emulator, the tag emulator including data corresponding to a plurality of first tags.

24. The system of claim 1, further comprising a data interface, for enabling communication with an external system.

25. The system of claim 1, further configured to require online authentication prior to reading or writing to a tag using a unique identifier associated with the system.

26. The system of claim 1, further including a single tag holder associated with both the wireless access tag reader and the wireless access tag writer.

27. The system of claim 1, further including separate tag holders associated with the wireless access tag reader and the wireless access tag writer respectively.

28. The system of claim 1, configurable to write multiple copies of a tag without re-reading the first wireless tag.

29. A wireless access tag duplication device comprising:

a wireless access tag reader;

a wireless access tag writer;

a processor, coupled to the wireless access card reader and the wireless access card writer; and

a memory, including instruction code, executable by the processor, for:

determining a first key of a first wireless access tag;

determining remaining keys of the first wireless access tag using nested authentication and the first key;

reading data of the first tag using the wireless access card reader, the first key and the remaining keys; and

writing the data to a second tag using the wireless access card writer, the first key and the remaining keys.

30. A wireless access tag duplication method comprising:

determining a first key of a first wireless access tag;

determining remaining keys of the first wireless access tag using nested authentication and the first key;

reading data of the first tag using a wireless access card reader, the first key and the remaining keys; and

writing the data to a second tag using a wireless access card writer, the first key and the remaining keys.

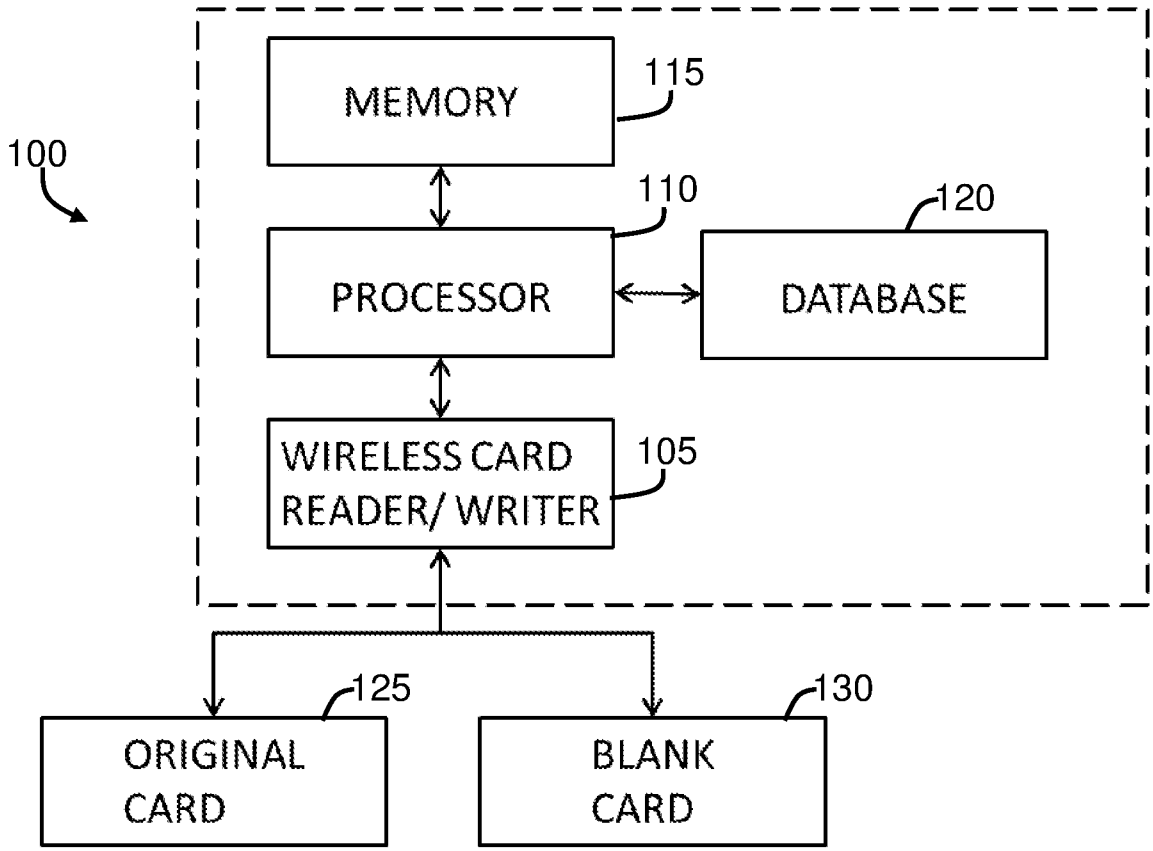

Figure 1

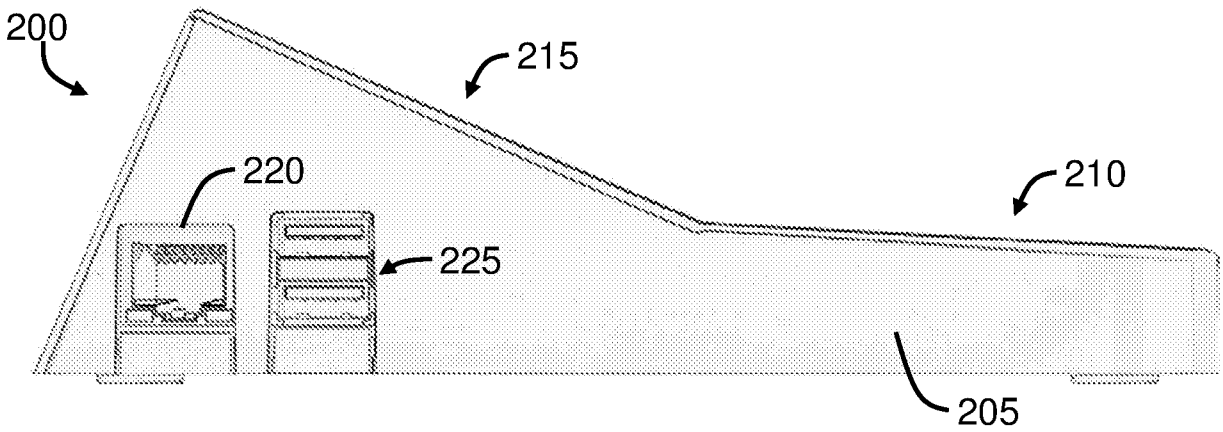

Figure 2b

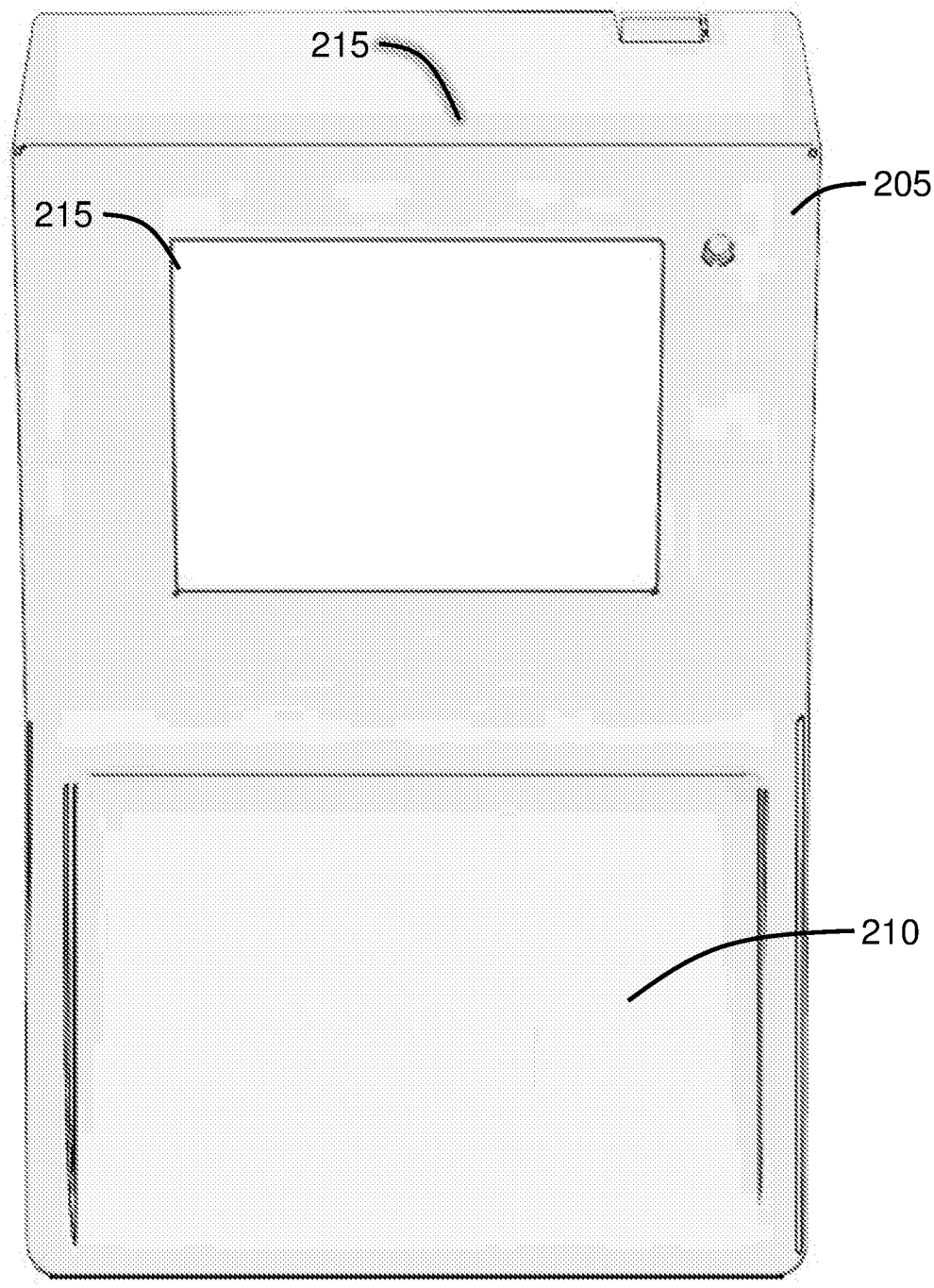

Figure 2a

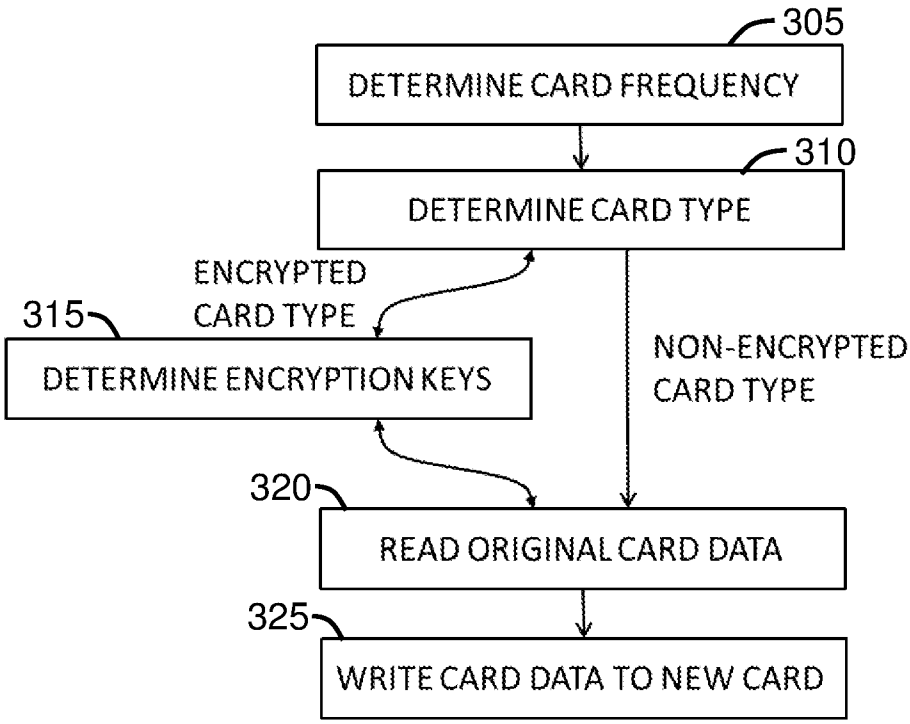

Figure 3

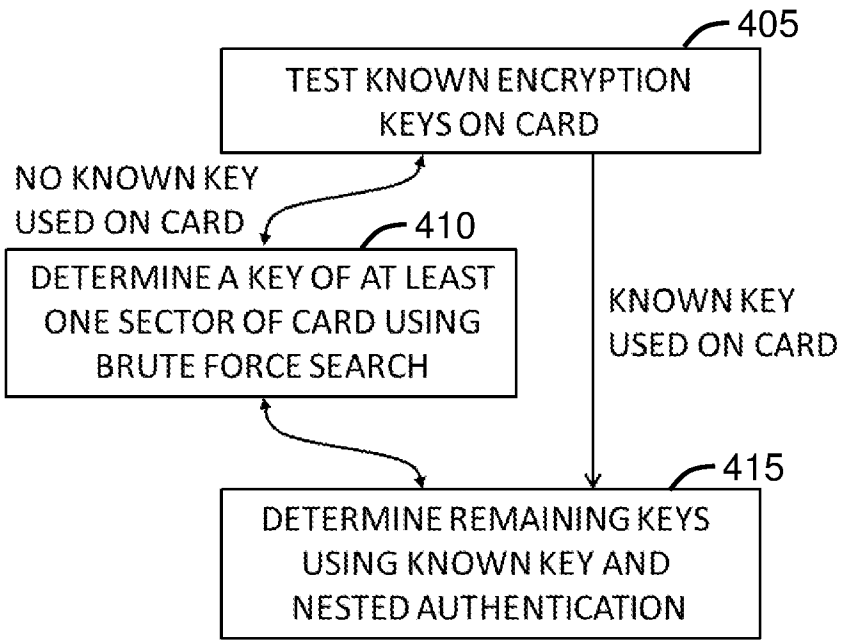

Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2016/050420

A. CLASSIFICATION OF SUBJECT MATTER

H04B 5/02 (2006.01) G06K 19/00 (2006.01) G06F 21/00 (2013.01)

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)

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)

Databases: EPODOC, WPIAP, INSPEC, GOOGLE, GOOGLE SCHOLAR and GOOGLE PATENTS and Espacenet

IPC/CPC marks: H04B5/02, G06K19/00 and G06F21/00

Keywords: Access tag, MIFARE, RFID, duplicate, clone, read, write, key, processor, hack, nested authentication, brute force search , first, second, key and similar terms.

Espacenet, AUSPAT and IP Australia internal databases: Applicant/Inventor name search

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C [X] 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
5 September 2016	05 September 2016
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Vinod Menon AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. 0262832763

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/AU2016/050420**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Márcio Almeida; "Hacking Mifare Classic Cards"; Black Hat Regional Summit, Sao Paulo; 25-26 November 2014 URL: https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf page 5, 12, 20-23, 34-36	1-30
X	YA LIU et al.; "Legitimate-reader-only attack on MIFARE Classic"; Mathematical and Computer Modelling; pages 219-226; Volume 58, Issues 1-2, July 2013 whole document, especially abstract, section 2: Preliminaries; sec 3: Main Results	1-30
X	WO 2008/145199 A1 (BIANCHI 1770 S.P.A) 04 December 2008 Whole document, especially abstract, page 4-5, 9, fig 1, 4	1-30
X	Gerhard de Koning Gans et al.; "A Practical Attack on the MIFARE Classic"; IFIP International Federation for Information Processing, CARDIS 2008; pages 267-282; 2008 Whole document	1-30

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2016/050420**

This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
WO 2008/145199 A1	04 December 2008	WO 2008145199 A1	04 Dec 2008
		IT PN20070040 A1	30 Nov 2008

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.