



(51) International Patent Classification:

G07C 9/00 (2020.01) E05B 67/22 (2006.01)
E05B 47/00 (2006.01)

(21) International Application Number:

PCT/IB2020/061882

(22) International Filing Date:

14 December 2020 (14.12.2020)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

19133604.9 13 December 2019 (13.12.2019) HK

(71) Applicant: **BRILLIANT GUARD LIMITED** [CN/CN];
Room 1305-1306, Leader Industrial Centre, 57-59 Au Pui
Wan Street, Fo Tan, Shatin, New Territories, Hong Kong,
Hong Kong (CN).

(72) Inventor: **KO, Ping Hon**; 2nd Floor, No. 260 Tin Sum
Village, Shatin, New Territories, Hong Kong, Hong Kong
(CN).

(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, IT, 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, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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 the applicant's entitlement to claim the priority of the
earlier application (Rule 4.17(iii))
- of inventorship (Rule 4.17(iv))

(54) Title: INTELLIGENT LOCKS AND KEYS

100

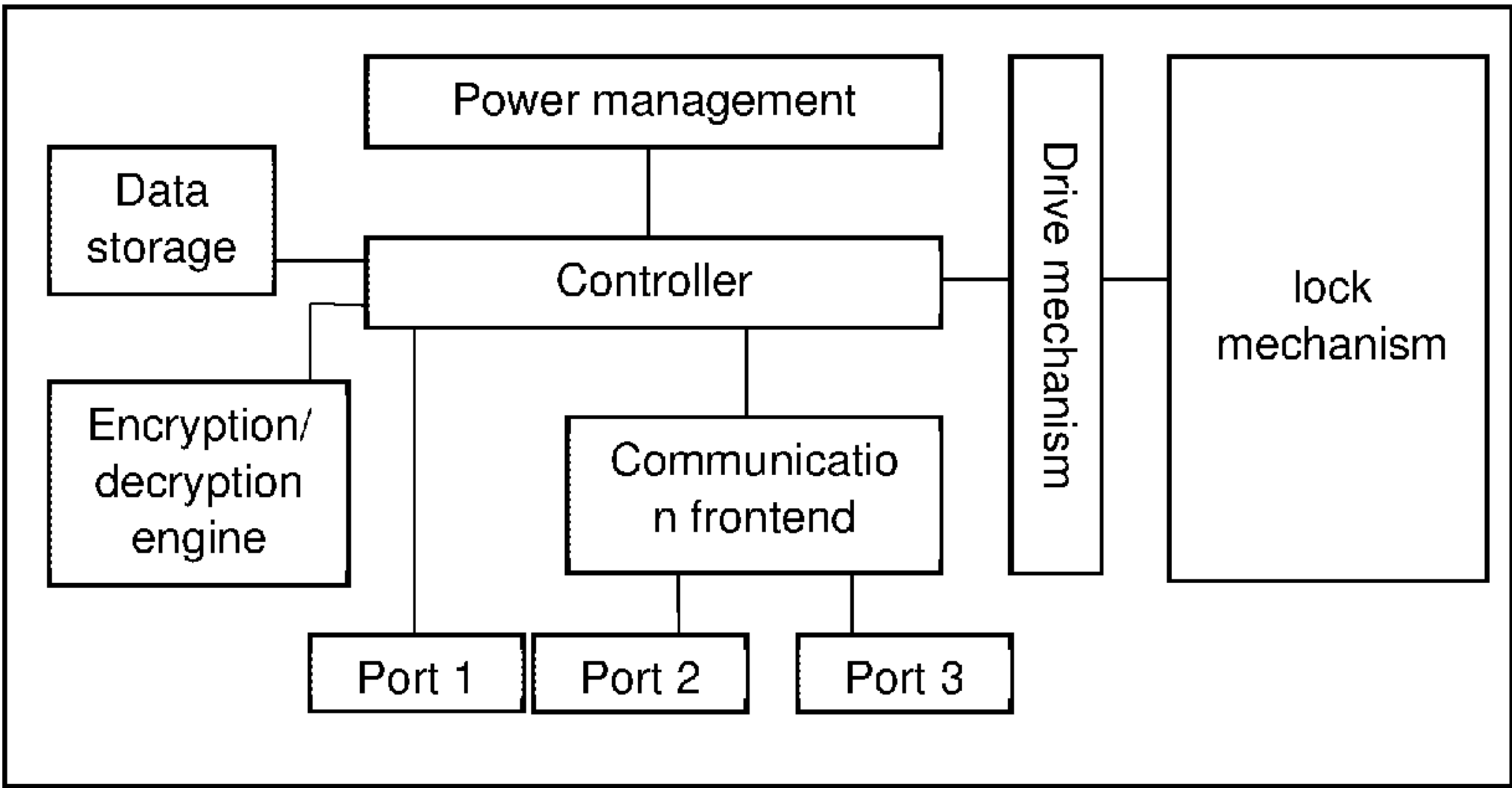


Fig. 1

(57) Abstract: The lock(100) comprises a controller, a data storage device, a lock mechanism operable by the controller in a locked state or an unlocked state, and a data communication frontend comprises a first data port(108) and a second data port; Wherein the controller is configured to enter into data communication via second data port after successful completion of data communication via the first data port(108). An electronic key(200) comprises a key controller, a data storage device, a power source and a data communication frontend comprising a first data port(202) and a second data port; wherein the electronic key(200) is a physical key having a key body and is configured to work with the lock(100).

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

INTELLIGENT LOCKS AND KEYS

Field of Disclosure

[001] The present disclosure relates to intelligent locks and intelligent keys, and more particularly to locks having a lock mechanism operable by intelligent electronic circuitry and electronic keys therefor.

Background

[002] Intelligent locks are electronic locks having a lock mechanism which is operable by electronic circuitry. Electronic locks enjoy increasing popularity because of its flexibility and enhance security. With the increasing use of intelligent locks, improved intelligent locks and keys are advantageous.

Summary of Disclosure

[003] A lock comprising a controller, a data storage device, a lock mechanism operable by the controller in a locked state or an unlocked state, and a data communication frontend comprising a first data port and a second data port is disclosed. The controller is configured to enter into data communication via the second data port after successful completion of data communication via the first data port.

[004] The controller may be configured to receive identification data via the first data port and to receive operational data messages via the second data port, and wherein the controller may be configured to not to receive operational data messages via the second data port if the identification data received via the first data portion does not meet an admission criterion.

[005] The controller may be configured to conduct unencrypted data communication via the first data port and encrypted data communication via the second data port.

[006] An electronic key configured to work with the above lock is disclosed. The electronic key comprises a key controller, a data storage device, a power source and a data communication frontend comprising a first data port and a second data port. The electronic key is a physical key having a key body.

[007] The key controller may be configured to send identification data via the first data port and to transmit operational data messages via the second data port after a positive response indicating admissibility is received via the first data port.

Description of Figures

[008] The present disclosure is described by way of example and with reference to the accompanying figures, in which:

[009] Figures 1 and 1A are block diagrams of example locks of the present disclosure,

[010] Figures 2 and 2A are block diagrams of example hard keys of the present disclosure,

[011] Figure 3 is a schematic diagram showing an example encryption process of a command message,

[012] Figures 4A is a front view of an example lock,

[013] Figure 4B is a perspective view showing an USB port of the example lock of Figure 4A,

[014] Figure 4C is a cross-sectional view of the example lock of Figure 4A,

[015] Figures 5A, 5B and 5C are front, perspective and cross-sectional views of an example hard key,

[016] Figure 5D is an exposed view of the example key of Figure 5A,

[017] Figure 6 shows interface ports of the example lock of Figure 4A and the example key of Figure 5A,

[018] Figures 7A and 7B are cross-sectional views showing the example lock and key of Figures 4A and 5B in mechanically coupled engagement in a latching position and a releasing position respectively,

[019] Figure 8 shows, schematically, remote operation of the example lock of Figure 4A by a data communication apparatus,

[020] Figure 9 shows, schematically, contact operation of the example lock of Figure 4A by a hard key in mated engagement with the lock,

[021] Figure 10 shows a flow chart of the operation of the example lock of Figure 4A by a hard key in mated engagement with the lock,

[022] Figure 11 shows, schematically, contactless operation of the example lock,

[023] Figures 12A, 12B, 13A and 13B show example safebox and lockbox forms of lock according to the disclosure, and

[024] Figures 14A, 14B, 15A and 15B show example cable lock and door lock forms of lock according to the disclosure.

Detailed description

[025] A lock of the present disclosure comprises electronic circuitries including a controller, a data storage device, a lock mechanism operable by the controller, a data communication frontend comprising a first port which is a first data communication port and a second port which is a second data communication port, as shown in Figure 1. The controller is a lock controller, which may comprise a microprocessor-based solid-state controller (MCU) which is configured to control the lock, including the settings and operations thereof, and peripheral circuitries configured to support operation of the MCU. The data storage device is for storing digital data, especially data in relation to the settings and operations of the lock, and may comprise volatile memories such as RAM and/or non-volatile member such as ROM or EPROM. The data storage device is in data communication connection with the controller so that data can be stored in the data storage device by the controller, and data stored in the data storage can be retrieved by the controller. The lock mechanism is operable in a first state in which the lock is in a locked state and a second state in which the lock is in an unlocked state. The data communication frontend, including the data ports thereof, is in data communication connection with the controller and is configured to facilitate data communication between the lock and an external device such as a key in cooperation with the controller. The electronic circuitries may comprise peripheral circuitries such as analog-to-digital converter, power management circuits, and other optional circuitries. The data communication herein means electronic data communication and may be wired and/or wireless. To facilitate wireless data communication, the electronic circuitries may comprise a wireless data transceiver.

[026] The first port is a data communication port which is configured for data communication of a first type of data and the second data port is a data communication port which is configured for data communication of a second type of data different to the first, and the difference between the first and second data types may be in data nature, data format, data speed and/or data modulation.

[027] In example embodiments, the lock controller is configured to perform a first procedure via the first data port prior to entering into a second procedure via the second data port. The first procedure may be a validation procedure during which the controller operates to determine whether data coming in from the first data port meet validation requirements. If outcome of the validation procedures is positive, that is, successful, the in-coming data is determined by the controller as coming in from an eligible object and the lock controller will proceed to the second procedure. If outcome of the first procedure is negative, that is, unsuccessful, the lock controller will not proceed to the second procedure.

[028] The lock may comprise a third port and the controller may be configured to perform a pre-procedure to determine whether or not to proceed to the first procedure with reference to a signal

present at the third port. If the signal present at the third port corresponds to signal of an eligible electronic key, the lock controller will operate to proceed to the first procedure. Otherwise, the lock controller will not proceed to the first procedure.

[029] The lock is configured to work with a key. In example embodiments, a key which is configured to work with a lock would have the identification parameter and the Encryption Key prestored on the key.

[030] The key can be a physical key or a software key which is configured to operate the lock by way of data communication. A software key is a non-dedicated electronic key which is generated by way of execution of application software which is resident on a host machine such as a smart phone, a tablet computer, a notebook computer, a personal computer, and other general-purpose or specific-purpose computer-based machines, and to operate the lock by way of wireless data communication. A physical key is a dedicated electronic key which is configured to operate the lock and the data communication may be wired and/or wireless. A host machine when executing the application software will become an application machine (“**APP**”) having an interface to work with the lock, including sending lock operation instructions and administrative instructions such as key reset.

[031] A physical key comprises electronic circuitries including a controller, a data storage device, a data communication frontend comprising a first data port and a second data port, and a key body, as shown in Figure 2. The first data port of the key is configured to perform data communication with the first data port of the lock and the second data port of the key is configured to perform data communication with the second data port of the lock. Since the first data ports of the key and the lock have to be mutually compatible and the second data ports of the key and the lock have to be mutually compatible, the description on and in relation to controller, the first and second types of data, the data ports, the data storage device, the telecommunication frontends, the controller, etc. are incorporated by reference and to apply mutatis mutandis to the key, for example, with the lock controller renamed as the key controller. Likewise, the description on and in relation to the first procedure, the second procedure, the third procedure, and the third port are incorporated by reference and to apply mutatis mutandis to the key.

[032] The first procedure may be a validation procedure which is designed to determine whether a key is configured for a target lock and whether a target lock has been paired with a key. If the outcome of determination is positive, the key is a qualified key, and the lock and the key are a qualified pair.

[033] The second procedure may be an instruction procedure during which a lock instruction or a plurality of lock instructions are to be sent to the lock, and the lock controller is configured to react to the instruction or instructions upon receipt.

[034] During the first procedure, the key may send an identification parameter to the lock and the lock upon receipt of the identification parameter will determine whether the identification parameter is correct. If the lock controller determines that the identification parameter is correct, the first procedure is successful and the controller will send an acknowledgement response.

[035] If outcome of the first procedure is positive, that is, successful, the lock controller will proceed to the second procedure, that is, to receive lock instructions via the second data port. If the outcome of the validation procedures is negative, that is, unsuccessful, the key is a non-eligible key and the lock controller will not send an acknowledgement response, and will not proceed to the second procedure, that is, the controller will operate to ignore data coming in from the non-eligible key.

[036] The identification parameter of the lock may be stored on the lock, for example, at time of manufacture, that is, ex-factory, to facilitate the validation procedure. The identification parameter should be unique to the lock and may be assigned by the manufacturer, for example, a serial number. The MAC address of the lock may be used as an identification parameter of the lock since the MAC address is recognized as a unique identification of a device.

[037] The third port may be configured as a compatibility signal port for reception of a compatibility signal. If a compatibility signal is detected at the third port, the controller will proceed to the first procedure. For example, the third port of compatible key may be set at a specific voltage and the lock controller on detecting that the specific voltage or a voltage within a specific voltage is present at the third port of the key will make the determination that the key has a valid compatibility signal to be eligible to proceed to the second procedure. Likewise, the third port of compatible lock may be set at a specific voltage and the key controller on detecting that the specific voltage or a voltage within a specific voltage is present at the third port of the lock will make the determination that the lock has a valid compatibility signal to be eligible to proceed to the second procedure.

[038] To determine whether a key is an eligible key having a valid compatibility signal, the third port of an eligible key and the third port of an eligible key lock may be configured to make physical and electrical contact so that the voltage of the third port of the key can be measured by the lock controller and vice versa.

[039] When determining whether a key has a valid compatibility signal, the third port of the lock may have an isolation switch which is operable by the controller to connect the third port with the power circuit of the lock or to isolate the third port from the power circuit, and the lock controller may operate the isolation switch to isolate the third port of the lock from the power circuit when taking signal measurements at the third port to avoid conflict. Likewise, the third port of the key may have an isolation switch which is operable by the controller to connect the third port with the power circuit of the key or to isolate the third port from the power circuit, and the key controller may operate the isolation switch to isolate the third port of the key from the power circuit of the key when taking signal measurements at the third port to avoid conflict.

[040] Data communication between a lock and a key is by way of data packets. An example data packet has 16-bytes of data and each byte has 8 bits of binary data. The data packets comprise two types of data packets, namely, a first type which is referred to as a command packet (“**Command Packet**”) and a second type which is referred to as a response packet (“**Response Packet**”) which is configured to respond to a received command packet.

[041] An example command packet comprises an overhead portion and a payload portion. An example command packet has a 11-byte payload portion (say byte 3 to byte 13) and a 5-byte overhead portion (say bytes 0-2 and bytes 14-15). The payload portion comprises an “array” type data portion containing command parameters and the overhead portion comprises a command packet sequence number (SEQ, 2 bytes), type information (“CMD”, command) and a 2-byte checksum (“CSM”).

[042] An example response packet comprises an overhead portion and a payload portion. An example command packet has a 10-byte payload portion (say byte 4 to byte 13) and a 6-byte overhead portion (say bytes 0-3 and bytes 14-15). The payload portion comprises an “array” type data portion including response parameters and the overhead portion comprises a response packet sequence number (RSEQ, 2 bytes), type information (“RCM”, response), an error field (“ERR”, 1 byte) to indicate whether the received command has been successfully performed, and a 2-byte checksum (“CSM”).

[043] A command is an instruction which may be classified as a lock operations command, an administration command (or admin command), or an inquiry command. A lock operation instruction is one which is configured to instruct the lock controller to perform lock operations such as locking and unlocking. An administration command is one which is configured to instruct the lock controller to set parameters such as clock time, motor forward time, motor reverse time, timers such as advertising intervals, advertisement disabling time, etc. An inquiry command is

one which is configured to instruct the lock controller to return status information of the lock and may comprise commands to get lock status (locked, unlocked, damaged), lock operation records, etc.

[044] A lock instruction may be encrypted to facilitate secured data communication between a key and a corresponding lock which is paired with the key. To facilitate secured data communication, the controller may comprise an encryption and decryption machine. The encryption and decryption machine may be an electronic circuit which is dedicated to perform data encryption and data decryption, for example, according to a data encryption algorithm such as one complying with AES (Advanced Encryption Standard). In example embodiments, the AES 128 standard using 128-bit data (that is, 6-byte data) is employed. To facilitate data encryption and decryption, a data encryption and decryption key is stored in the lock. The data encryption and decryption key ("**Encryption Key**" or "**Decryption Key**") may be stored at the time of manufacture or may be installed and stored on the lock by user's initiation post-purchase.

[045] During operations, a user may operate a key to send instructions to the lock via the second data port only. The lock controller upon detection of the instructions will operate in accordance with data contents of the instruction. Where the lock is configured to operate with secured data communication and encrypted instructions, the lock controller will operate to decrypt the encrypted instruction received and to operate according to the decrypted instruction. Where the lock controller is configured to send a response to the key in response to a received instruction, the lock controller will respond by sending a response command or an encrypted response command via the second data port. When an encrypted response command is received, the key controller will operate to decrypt the received encrypted response command and to update lock status where appropriate.

[046] The second data port may be configured for wireless data communication and day-to-day operations of the lock may be by way of wireless data communication via the second data port only, for example when the encryption key is already saved on the lock.

[047] A software key is configured to operate the lock by way of data communication via the second data port only, for example, by wired or wireless data communication.

[048] The lock and a paired key may be configured for Bluetooth (RTM) operations, for example, via the second port. A Bluetooth (RTM) enabled controller such as the TC35680FSG/TC35681FSG of the Toshiba Corporation may be used as the lock controller and the key controller as a convenient example. The example controller is configured for BTLE

(Bluetooth (RTM) low energy operation protocol) version 5.0 and is to operate at 2.4GHz. To be compliant with BTLE protocols, each lock command is preceding by an UUID (universally unique identifier). Of course, the command data format will be different if a different wireless data communication standard is used. In example embodiments, the second data port of the lock may be configured for wireless data communication only.

[049] To operate a lock by a software key which is resident on a host machine, the host machine on execution of the application software will look for the lock to pair, and the pairing can be performed by connection protocols of the communication standard as the identification information of the lock is unknown. After connection has been established, the host machine will send lock instructions to the lock and the lock controller will respond by broadcasting response commands via the second data port, and to perform lock operations where appropriate. When the lock instructions and the response commands are encrypted, the respective controllers will perform decryption to retrieve the embedded data.

[050] To facilitate contact operation of a lock by a physical key, the lock is provided with a key interface and the key is provided with a lock interface which is configured for mated physical engagement with the key interface. The key interface comprises a plurality of terminals including a first terminal which is configured as a first data port and a second terminal which is configured as a third port which is compatibility signal port.

[051] In example embodiments, both the lock interface and the key interface are configured to be physically compatible with the USB micro-B connector standard, although one is configured as a female connector and the other one is configured as a male connector.

[052] The USB connector has 5 terminals, namely terminals 1 to 5. Terminal 1 is configured as a positive voltage terminal which is to be set at a positive voltage V_{CC} , terminal 2 is a negative data terminal, terminal 3 is a positive data terminal, terminal 4 is an identification (ID) terminal, and terminal 5 is a reference terminal which is set a ground potential. The positive voltage V_{CC} is rated at 5V, but actual voltage may vary between 4.4V and 5.25V. The positive data terminal is configured as the first data port or data port 1 while the ID terminal is configured as the third port or the compatibility signal port. The ID terminal is configured to be biased at a compatibility signal level, and the compatibility signal level may be different to V_{CC} , for example, 3.675V.

[053] In example embodiments, after the physical key has entered into physical and electrical engagement with the lock, the lock controller will perform the pre-procedure via the ID terminal

and then the first procedure via the first data port. The first procedure may be performed using USB data communication protocol.

[054] During execution of the first procedure, the key may send the identification parameter of the lock to look for presence of the lock. When the lock receives an incoming data message corresponding to an incoming inquiry looking for presence of the lock, the lock on detecting its own identification parameter will send an acknowledgement response which may include its identification parameter to show presence. In example embodiments, the MAC address is used as the identification parameter since a MAC address is sufficiently unique, and the identification parameter sent is not encrypted.

[055] A physical key or a host machine may include a plurality of softkeys for operating a corresponding plurality of locks and a user may select one of the stored softkeys to pair with a target lock in order to enter into lock instruction data communication with the target lock.

[056] After completion of the first procedure, the lock controller will advertise using BLTE protocol and the physical key will establish data communication connection with the lock whereby lock instructions are sent by the key controller and response commands are sent by the lock controller, all via the second data port and by means of wireless data communication.

[057] In a secured version of the lock, the lock instructions and the response commands are encrypted using the Encryption Key.

[058] In example embodiments, the encryption key (and the decryption key) used by the physical key has a higher authorization level and is different from the encryption key (and the decryption key) used by a host machine. An encryption key having the higher authorization level is referred to herein as an Admin key and the encryption key used by the host machine has a lower authorization level and is referred to as a User Key. Admin commands may be available to an Admin Key but not a User Key to avoid conflict or to enhance lock security.

[059] In example embodiments, the lock will require an Admin Key encrypted lock instruction on detecting that a physical key is in data communication with the lock via the first data port, and to ignore User Key encrypted lock instructions on detecting that a physical key is in data communication with the lock via the first data port.

[060] In example embodiments, data communication via the first data port and data communication via the second data port use different communication standards or protocols. For example, data communication via the first data port may follow USB protocol or NFC protocol while that on the second data portion may be in accordance with Bluetooth (RTM) protocol.

[061] In example embodiments, the physical key is configured to provide operating power to the lock when the physical key is in physical and electrical contact with the key interface of the lock. For example, when the lock detects a physical key in physical engagement with its key interface, the lock controller may operate to switch the power management circuitry so that lock mechanism operating power is supplied by the physical key, rather than by internal stored power of the lock.

[062] Where the lock is configured for more secured operation, the physical key is equipped with the Admin Key and lock instructions which are transmitted via the second data port are encrypted with the Admin Key. If the physical key having the Admin Key is removed from physical connection with the key interface after completion of the first procedure and before completion of the second procedure, the lock controller is configured to operate to abort the second procedure. The lock controller may be configured to constantly monitor the compatibility signal port in order to determine continued presence or absence of the physical key.

[063] In example embodiments, that the physical key carries an Admin Key may be readily known by the lock, for example, the identification parameter of the physical key may have been stored on the lock's database.

[064] The User Key or the Admin Key ("**Key**" collectively) may be pre-stored in the lock and may be made available to the lock retrospectively. A Key which is made available retrospectively is beneficial, for example, the Key may be changed when ownership of the lock changes.

[065] The Key may be set or reset by cooperation between a master key, a host machine running the APP and a server. A master key may be a physical key which is prestored with a default key and the identification parameter of the lock. The default key and the identification parameter of the lock are also stored on the lock and a server which hosts the default keys of many locks. The default key ("**Default Key**") is an encryption key, or more specifically, a reserved encryption key which is reserved for setting an Admin Key and User Keys.

[066] In order to retrospectively get a KEY, the host machine will need to communicate with the server with an aim of getting the KEY. The information provided by the host machine to the server will include the identification parameter of the lock such as its MAC address. MAC address is used as a convenient example of an identification parameter in the present example and reference to MAC herein may be construed as reference to identification parameter where appropriate. Upon receipt of the request, the server will return a KEY which is encrypted with the Default Key to the host machine. After the host machine has received the Default Key encrypted

KEY, the host machine will forward the encrypted Key to the lock and the key and the lock and the key will retrieve the KEY by decryption using the Default Key.

[067] The encrypted Key may be sent by a command Set_Key_Req and the lock controller or key controller from the UUID of the command will realize that this is a Key setup command and will use the Default Key to retrieve the KEY, which is a second encrypted key while the default key is a first encrypted key.

[068] An example lock **100** comprises a lock mechanism, a drive mechanism, electronic circuitries comprising a controller and peripheral circuits including an encryption/decryption engine, a wireless data communication frontend, a key interface, a power management circuit and a main housing, as depicted in Figure 1A.

[069] The wireless data communication frontend is configured for wireless transmission and wireless reception of data and comprises a radio-frequency transceiver (TX) and an antenna, and. The radio-frequency transceiver is electrically connected intermediate the controller and the antenna so that the controller can receive and transmit data via the antenna.

[070] The lock mechanism comprises a latching mechanism which is operable between a first state which is a locked state and a second state which is an unlocked or open state. When the lock mechanism is in the locked state, the latching mechanism is in physical engagement with a latching port. When the lock mechanism is in the unlocked state, the latching mechanism is disengaged or released from the latching port.

[071] The drive mechanism is configured to drive the lock mechanism to move between the locked state and the unlocked state and its operation is controlled by the controller.

[072] The controller of the lock (or lock controller) is configured to send and receive instructions to the drive mechanism to operate the lock mechanism, to receive data, to process received data, to retrieve data, to transmit data, to send control signals to operate the drive mechanism, and to perform other control, communication and data processing functions without loss of generality.

[073] The key interface is optional and is configured to interact with a physical key, for example a hard key of the present disclosure which is a physical key, and comprises a key portal which is a key interface port.

[074] The controller comprises a solid-state microprocessor having built-in memory and peripheral circuitry. The memory comprises volatile memory and non-volatile memory and the

controller may be realized as a control circuit comprising a microprocessor and peripheral circuitry and memory.

[075] The power management circuit is configured to manage power supply for operation of the lock. Where the lock is a portable lock, the power management circuit comprises a portable power source such as a battery, in particular a rechargeable battery such as a lithium ion battery, a charging circuit for charging the power source, and optionally a battery charging port for connection with a charging power source. Where the lock is a fixture lock, the power supply may comprise a rectifier circuit for converting AC mains power to DC operation power. A fixture lock herein means the lock as mounted as a fixture and forms part of a fixture, such as part of a door or gate.

[076] The power management circuit may comprise a power selector which is to select a power source from a plurality of available power sources. For example, the power selector may be configured to select an external power such as power from a hard key when the hard key is in keyed connection with the lock. The power selector may comprise a power switch which is operable by the controller to switch supply power to the lock mechanism between the power sources.

[077] The main housing may be constructed of a robust and tamper resistant material and defines an internal compartment inside which components such as the electronic circuitry and power supply are housed.

[078] The latching port is formed on or mounted inside the main housing and may have a rigid indented portion where the key interface is configured as a female connector.

[079] A movable portion of the latching mechanism is hidden inside the main housing and a movable portion of the latching mechanism is exposable from the main housing. For example, the latching port is inside the main housing and a movable portion of the latching mechanism is exposed outside the main housing when in the locked state. The movable portion may retreat or advance towards the main housing to release physical engagement with the main housing when changing from the locked state to the unlocked state. The movable portion may comprise a pivoted hook in example embodiments of a portable lock and may comprise a latch in example embodiments of a fixture lock.

[080] The lock controller is configured to receive instructions, to process received instructions and to perform operations according to the received instructions. The instructions are exchanged between the lock and a corresponding apparatus by way of data communication schemes through

a data communication channel. The instructions are in the form of data messages and each data message is a command message (or message in short). Each message is a data string and the message is preferably an encrypted message to enhance security. Upon receipt of an encrypted command message or command messages, the controller is to operate to decrypt the message or messages and retrieve the embedded instructions. The AES 128-ECB encryption and decryption algorithms may be used as example encryption and decryption algorithm.

[081] The command messages may have different properties or characteristics and are categorized according to the function or purpose of the message.

[082] In example embodiments, the controller is configured to receive and process an example plurality of three categories of operation instructions, namely, a first category of user-oriented messages (or “**user messages**” in short), a second category of administration-oriented messages (or “**admin messages**” in short), and a third category which is a reset message for resetting the lock to factory settings.

[083] For example, a user message has user message characteristic and is configured to deliver operation instructions such as “open lock”, “close lock”, etc. An admin message is configured to deliver administrative instructions such as setting operation parameters, operation settings, get log records or other data such as date and time information and battery status.

[084] A user message may be encrypted with a user key (symbol: “**USR_KEY**”) or an admin key (symbol: “**ADM_KEY**” or “**admin key**” in short), and an admin message is encrypted with an admin key).

[085] Each lock has a unique identity and no two locks are configured to have the same identity. The unique identity is intended to serve as a means of identification of the lock and may be built-in at the time of manufacturing. The unique identity may be in the form of an identification code for machine recognition of the identity of the lock. MAC (Media Access Control) of the lock, for example, the MAC address of the controller, may be conveniently used as an identification code of the lock.

[086] An identification code of the lock may be imprinted on an outer surface of the lock or may be separated from the lock. The identification code may be presented in a machine-readable code such as a QR code, a bar code or other forms of digital codes. The identification code may be encrypted, for example, by encrypting a hashed MAC address using a softkey.

[087] The lock is operable by a hard key or by a softkey. A softkey herein is an intangible key which is configured as a data string for operation of the lock, for example, to change a lock from

a locked state to an unlocked state or to change from the unlocked to locked state. An example softkey herein is a data string having an example data sequence of an example plurality of 128 binary data bits. The softkey may be transmitted as a string of electrical data signals by the hard key or by an apparatus ("APP") pre-stored with a softkey and having a wireless data transmitter.

[088] A hard key herein is a tangible key. The hard key comprises a lock interface for making physical contact or engagement with a corresponding key interface on the lock and comprises a lock interface port.

[089] An example hard key **200** for operation with the lock comprises a controller, a wireless data communication frontend, a lock interface, a power source, a power management circuit and a main housing, as depicted in Figure 2A.

[090] The lock interface comprises a lock portal which is configured to physically interact with the key portal of the lock. The lock portal is configured to be physically compatible with the key portal of the lock. In example embodiments, the key portal and the lock portal are complementarily shaped. For example, the lock portal may have a first profile and the key may have a second profile which is physically complementary to the first profile. In example embodiments, the lock portal comprises a protrusion portion having a first physical profile and the key portal has a receptacle defining a compartment and having a second physical profile which is physically complementary to the first physical profile.

[091] The wireless data communication frontend comprises a radio-frequency transceiver (TX/RX) and an antenna, and is configured for wireless transmission and wireless reception of data.

[092] The radio-frequency transceiver electrically is connected intermediate the controller and the antenna so that the controller can receive data from the antenna and can transmit data from the antenna to the ambient.

[093] The controller of the hard key (or key controller) is configured to send instructions to the lock, to receive data from the lock, to process received data, to retrieve data, and to perform other control, communication and data processing functions without loss of generality.

[094] The controller comprises a solid-state microprocessor having built-in memory and peripheral circuitries. The memory may comprise volatile memory and non-volatile memory and the controller may be realized as a control circuit comprising a microprocessor and peripheral circuitries and memory.

[095] The power management circuit is configured to manage operation power of the hard key and comprises a charging circuit for charging the power source. The charging circuit is connected to a battery charging port having a connection interface on the main housing for physical connection to a battery charging power source. In example embodiments such as the present, the battery charging port is adjacent to the lock interface and is in an optional form of a USB micro-B female connector. The power source of the key is also configured to supply power for operation of the lock in some circumstances, for example, when the lock and the key are in keyed physical connection. When a lock and a key are in keyed connection herein means when they are in complementary physical connection. The power source of the key may be a rechargeable battery, for example, a lithium battery comprising one battery cell or a plurality of battery cells, such as CR2032 button cells.

[096] Each lock has a built-in softkey which is affixed or embedded in the lock at the time of manufacturing. In example embodiments, the softkey is flashed into the non-volatile memory or ROM of the lock. The built-in softkey is a unique key of the lock and is conveniently referred to herein as a Default Key.

[097] Each lock has a hard key which is paired with the lock. The lock and the paired hard key, which is conveniently referred to as a Master Key herein, may be delivered to a purchaser at time of delivery or ex-factory.

[098] A copy of the Default Key is saved on the Master Key. The Default Key may be affixed on the Master Key at time of manufacturing. For example, the Default Key may be flashed into the non-volatile memory or ROM of the key.

[099] A copy of the Default Key is also stored on a secured host. The host may be a host server operating a host website to provide customer support or user support and has a database of locks, their characteristics and their Default Key. A copy of the Default Key may be downloaded from the host upon successful registration or upon satisfactorily meeting authentication requirements.

[0100] In example embodiments such as the present, the lock and the Master Key have no valid or useable User Key at the time of manufacturing or in the ex-factory state. In such embodiments, the User Key of the lock and the Master Key may be factory pre-set to an ex-factory default value such as nullity or **INVALID**. Likewise, the Default Key may be pre-set as the Admin Key in the ex-factory state. The default User Key and the default Admin Key may be replaced by a new User Key and a new Admin Key respectively when the lock is initialized.

[0101] For example, an initialization process is to be performed by a user when a lock is to be used for a first time by a user. To initialize the lock to operate, the user is to send an initialization request to the host server to request for activation of the lock. Upon receipt of the initialization request, the host server will send a set of softkeys to the owner in response. The set of softkeys may comprise a User Key and an Admin Key. Each one of the User Key and the Admin Key is a softkey. An example softkey herein is a coded data string formed by encryption of the Default Key, whether directly or indirectly. Upon receipt of the softkeys, the owner would then be able to operate the lock using the softkeys.

[0102] After the initialization process has been completed, the lock is ready for use by the user, who is in possession of the softkeys.

[0103] To operate the lock, a user will send an instruction to the lock. The lock on receipt of the instruction will respond to the instruction and perform the instruction accordingly.

[0104] An instruction may be a user instruction or an admin instruction. A user instruction is contained in a user message and an admin instruction is contained in an admin message.

[0105] A user message may be encrypted with a user key or the admin key while an admin message is encrypted by the admin key.

[0106] Upon receipt of the instruction, the lock will examine and determine whether the instruction carries a valid KEY. If the instruction carries a valid KEY, the instruction is taken as an authentic instruction and the lock will proceed to perform pre-defined operations according to the instruction.

[0107] An example message has four example message portions, namely, a first portion which is "Sequence number", a second portion which is "Command", a third portion which is "Data" and a fourth portion which is "CRC" (cyclic redundancy check). The example message has a 16-byte format and contains 128 binary data bits and is encrypted by a KEY to form an encrypted message, as shown schematically in Figure 3.

[0108] In example set-ups, a user is to use a data communication apparatus such as a smart phone to download application software ("**App**") from the host website. A data communication apparatus comprises a controller, a memory storage, a user-interface and a telecommunication frontend. The telecommunication frontend comprises a data communication frontend including a wireless data transceiver. The data communication apparatus may comprise a display such as a touch-panel screen. The example data communication apparatus may run on an operating system such as Android™ or iOS™.

[0109] After the App has been downloaded, the App is resident on the memory storage of the data communication apparatus as stored instructions and is ready for execution. The user may operate the data communication apparatus to execute the stored instructions to run the App and send an identification code of the lock to the host website to request for activation.

[0110] In example embodiments, the data communication apparatus comprises an image capture device such as a digital camera and the App includes an image capture and process routine. To initiate a request for activation, a user is to activate the App on the data communication apparatus. Upon activation of the App, the data communication apparatus is to operate to execute stored instructions to capture an image of the identification code, to process the image, and to retrieve the identification code from the processed image.

[0111] In some embodiments, the identification code is in human-readable form and the data communication apparatus comprises a user interface for a user to input the identification code. Upon receipt of the human readable identification code, the data communication apparatus running the App will determine authenticity of the identification code.

[0112] The host server on examination of the request and the identification code accompanying the request would on execution of stored instructions determine whether the received code is a genuine identification code of the lock. If the received code is determined to be a genuine or authentic identification code of the lock, the host server will transmit the softkeys to the requesting apparatus or an electronic account designed by the request. In some embodiments, the host server will transmit a copy of the softkeys to a designated or registered account as an alternative or in addition. Where the lock has been activated before, signifying a new user replacing an old user, the host server will deactivate previous or old softkeys and notify the lock of the change in status of the softkeys by sending the lock a copy of the new softkeys. The lock is notified of the change of user or owner, for example, upon receipt of the new softkeys, and will update its records, including de-activation or obsolescence of the old softkeys.

[0113] A copy of the softkeys may be stored on the hard key, on a smart phone or on a data communication apparatus configured to operate as an electronic key of the lock on user's choice or preference.

[0114] Data communication between the data communication apparatus and the lock may be in two example forms of data packets.

[0115] A first example form is a Command Packet having the example format shown in Table 1:

[0116] Table 1

Command Packet:

Offset	Field	Type	Size (byte)	Description
0	SEQ	BYTE	2	Sequence Number Starts with the next sequence number set in IDV / IDF command
2	CMD	BYTE	1	Command Code
3 “ “ “ “ 13	DATA	ARRAY	11	11 bytes of Command parameters. LSB first
14	CSM	BYTE	2	16-bit checksum. Sum of byte 0 to byte 13. Low byte first.

[0117] A second example form is a Response Packet having the example format of Table 2:

[0118] Table 2

Response Packet:

Offset	Field	Type	Size (byte)	Description
0	RSEQ	BYTE	2	Sequence Number of the command packet to be response
2	RCM	BYTE	1	Response Command Code = Command Code
3	ERR	BYTE	1	Status of Command Execution. 0x00 -> success
4 “ “ “ “ 13	DATA	ARRAY	10	10 bytes of response parameters.
14	CSM	BYTE	1	16-bit checksum. Sum of byte 0 to byte 13. Low byte first.

[0119] The lock is to send out a Response Packet upon receipt of a Command Packet.

[0120] The lock supports a plurality of services including, for example, device information, device service and other services. Each type of service has a universally unique identifier (**UUID**) plus a plurality of supported characteristics.

[0121] Device Information is configured to provide firm information of the lock. Firm information means data which are affixed or built in to the lock at manufacturing. The example Device Information Service uses a 16-bit UUID and includes a plurality of read only (“**R**”) information of the lock. The example readable information may include identity of the manufacturer, the model number of the lock, lock serial number, and other useful information such as hardware version, firmware version and software version .

[0122] The lock (**DEV**) supports a plurality of services and example services and some characteristics are shown in Table 3 below.

[0123] Table 3

Name	Data Direction	Property	Encryption	No. of bytes
Device Status	DEV → APP	R / N	NO	2
Reset Message	APP → DEV	WO / N	DEFAULT_KEY	16
User Message	APP → DEV	WO / N	USER_KEY	16
Admin Message	APP → DEV	WO / N	ADMIN_DEY	16
Device Configuration	APP → DEV	WO	None	16

[0124] The lock status is read-only and is configured to inform the host machine (or “**APP**”) the status of the lock, that is, whether the lock is in the locked state or in the unlocked or open state. The Lock Status has an example data length of one byte and has a binary value, for example, 1 or 0.

[0125] The Reset Message is an example Command Packet and is configured for resetting the lock to its ex-factory mode. When the lock is at its ex-factory mode, the lock is reset to its ex-factory settings. The Reset Message is a top-level control command requiring top-level security and is encrypted by the Default Key.

[0126] The User Message is an example Command Packet and is configured for operating the lock, for example, to change the lock from the locked state to the unlocked state and/or from the unlocked state to the locked state. The User Message is a user-level or operational-level control

command which is encrypted by the User Key or the Admin Key. The User Key (**USR_KEY**) is set to an example value of **INVALID** at the ex-factory state or at the ex-factory mode and may have an example 16-byte hexadecimal value.

[0127] Example of Command Messages having admin message characteristics are set out in Table 4 below.

[0128] Table 4

Instructions	Purpose
Set_timing	Set motor turning time FWD, REV
Get_timing	Get motor turning time FWD, REV
Set_admin_key	Set the Admin key into the lock
Set_User_Key	Set the User key into the lock
Get_User_Key	Get the User key from the lock
Set_RTC	APP to set real time clock of the lock
Get_RTC	Get the real time clock
Get_Lock_Record	Get the master key open lock record
Get_Total_Lock_Record	Get the number of record
Clr_Log	Clear the master key open log records
Identity_Verification	Perform an identity verification with the Lock, have to be first command sent that prevent other connection connect to the lock and not release.

[0129] The Open_Lock command is configured to be transmitted by the APP. The command has the example command and response data formats as depicted in Table 9 below.

[0130] Table 5

OPEN_LOCK Command

SEQ	2 bytes	Sequence Number	KEY
CMD	1 byte	0x59	ADMIN_K EY/ USER_KEY
DATA	4 bytes	= "APPO", if send through Admin Message Characteristic	

		= "USRO", if send through User Message Characteristic	
	1 byte	= 'L' -> open the shackle lock = 'D' -> open the door lock	
	6 bytes	"OPENLK"	
CSM	2 bytes	Check Sum	

Response

RSEQ	2 bytes	Response Sequence Number	ADMIN_KEY / USER_KEY
RCM	1 byte	0x59	
ERR	1 byte	ERROR CODE	
DATA	10 bytes	0x00	
CSM	2 bytes	Check Sum	

[0131] In response to the Command the lock controller will open the lock and sent a response to notify that the lock has opened.

[0132] The Open_Lock_Master_Key command is configured to be transmitted by the Master Key, and has an example format as shown in Table 6.

[0133] Table 6

OPEN_LOCK_MASTER_KEY Command

SEQ	2 bytes	Sequence Number	Key
CMD	1 byte	0x5A	USER_KEY
DATA	4 bytes	"KEYO"	
	1 byte	'L' -> open the shackle lock 'D' -> open the door lock	
	3 bytes	ID of the Master Key issuing this command These 3 bytes will be the least significant 3 bytes of the Master Key's BT device address. For example, the BT address of MASTER KEY is F4:04:4C:AA:BB:CC, then these 3 bytes will be {0xAA, 0xBB, 0xCC}	

	3 bytes	"MAS"	
CSM	2 bytes	Check Sum	

Response

RSEQ	2 bytes	Response Sequence Number	USER_KEY
RCM	1 byte	0x5A	
ERR	1 byte	ERROR CODE	
DATA	10 bytes	0x00	
CSM	2 bytes	Check Sum	

[0134] After the lock has been opened by the Master Key issuing the Open_Lock_Master_Key command, the time of lock opening and the identity of the Master Key will be logged by the lock and the logged date will be saved on the lock and retrievable.

[0135] The Set_timing Command is an administrative command which is to set the motor forward (FWD) time, to set the motor reverse (REV) time, or the disable advertisement timeout value. The command has the example command and response data formats as shown in Table 7 below.

[0136] Table 7

SET_TIMING Command

SEQ	2 bytes	Sequence Number	Key
CMD	1 byte	0x40	ADMIN_KEY
DATA	2 bytes (Little Endian Format)	Motor Forward time in mS Value from 100 – 2000 Other values are invalid	
	2 bytes (Little Endian Format)	Motor Reverse time in mS Value from 100 – 2000 Other values are invalid	
	1 byte	Disable advertisement time in minutes, value ranges from 0x00 – 0xFF. 0x00 – always enable Other values mean time to disable advertisement in minutes	
	6 bytes	"SETTIM"	

CSM	2 bytes	Check Sum	
Response			
RSEQ	2 bytes	Response Sequence Number	ADMIN_KEY
RCM	1 byte	0x40	
ERR	1 byte	ERROR CODE	
DATA	2 bytes (Little Endian Format)	Motor Forward time in mS Value from 100 – 5000	
	2 bytes (Little Endian Format)	Motor Reverse time in mS Value from 100 – 5000	
	1 byte	Disable advertisement time in minutes, value ranges from 0x00 – 0xFF. 0x00 – always enable Other values mean time to disable advertisement in minutes	
	2 bytes (Little Endian Format)	Average Motor Driving Current in mA	
	3 bytes	0x00	
CSM	2 bytes	Check Sum	

[0137] The Get_timing Command is an administrative command which is to get the motor forward (FWD) time, to set the motor reverse (REV) time, or the disable advertisement timeout value.

[0138] The Reset_Seq_Num Command is both an administrative command and a user command which is to re-initialize the sequence number and has an example format as shown in Table 8 below.

[0139] Table 8

RESET_SEQ-NUM Command

SEQ	2 bytes	Sequence Number	Key
CMD	1 byte	0x42	ADMIN_KEY
DATA	7 bytes	“RST_SEQ”	
	2 bytes	New Sequence Number 0xn timer	
	2 bytes	Inverted New Sequence Number -0xn timer	
CSM	2 bytes	Check Sum	

Response

RSEQ	2 bytes	Response Sequence Number	ADMIN_KEY
RCM	1 byte	0x42	
ERR	1 byte	ERROR CODE	
DATA	10 bytes	0x00	
CSM	1 byte	Check Sum	

The Set_Admin_Key Command is an administrative command which is to be used by the APP to set the Admin Key. The Admin Key is an important encryption key for encryption of admin messages and has an example data length of 16 bytes. The example process of setting a new Admin Key is divided into an example plurality of three phases. In the first phase, the APP is to send a first portion of the new Admin Key to the lock. The APP is to send a second portion of the new Admin Key to the lock upon receipt of a response message from the lock signifying that the first portion of the Admin Key has been received. Upon receipt of a response message from the lock signifying that the second portion of the new Admin Key has been received, the APP will then send a Set_Key_Finish to the lock to signify completion of new Admin Key setting. During the new Admin Key setting the old or existing Admin Key will be used for data encryption and decryption.

[0140] The lower 8 bytes of the new Admin Key are to be sent to the lock in the first phase, the upper 8 bytes of the new Admin Key are to be sent to the lock in the second phase after the lock has responded with an acknowledgement message, and a SETADMOK message is sent by the APP in the third phase. After the new Admin Key has been set, the new Admin Key will be used for subsequently until another new Admin Key is set.

[0141] The Set_User_Key Command is an administrative command which is to be used by the APP to set the User Key. The User Key is an important encryption key for encryption of User messages and has an example data length of 16 bytes. The example process of setting a new User Key is divided into an example plurality of three phases. In the first phase, the APP is to send a first portion of the new User Key to the lock. The APP is to send a second portion of the new User Key to the lock upon receipt of a response message from the lock signifying that the first portion of the User Key has been received. Upon receipt of a response message from the lock signifying that the second portion of the new User Key has been received, the APP will then send a Set_Key_Finnish to the lock to signify completion of new User Key setting. During the new User Key setting the old or existing Admin Key will be used for data encryption and decryption. The command has the example command and response data formats as depicted in Table 10 below.

[0142] Table 9

SET_USER_KEY Command

SEQ	2 bytes	Sequence Number	Key
CMD	1 byte	0x33	ADMIN_KEY
DATA	2 bytes	“UK”	
	1 byte	KEY_PHASE “1” – lower 8-bytes of new key “2” – upper 8-bytes of new key “9” – SET_KEY_FINISH Others - invalid	
	8 bytes	If KEY_PHASE = 0x31 (‘1’) Lower 8 bytes of key If KEY_PHASE = 0x32 (“2”) Upper 8 bytes of key If KEY_PHASE = 0x39 (“9”), Must set to “SETUSROK”	
CSM	2 bytes	Check Sum	

Response

RSEQ	2 bytes	Response Sequence Number	ADMIN_KEY
RCM	1 byte	0x33	
ERR	1 byte	ERROR CODE	
DATA	10 bytes	0x00	
CSM	2 bytes	Check Sum	

[0143] In the example as shown in Table 9, the lower 8 bytes of the new User Key are to be sent to the lock in the first phase, the upper 8 bytes of the new User Key are to be sent to the lock in the second phase after the lock has responded with an acknowledgement message, and a SETUSROK message is sent by the APP in the third phase. After the new Admin Key has been set, the new Admin Key will be used subsequently until another new Admin Key is set.

[0144] The Get_User_Key Command is an administrative command which is to be used by the APP to get the User Key from the lock.

[0145] An example physical lock **100** which is implemented in the form of a padlock is shown in Figure 4A. An example hard key which is paired with the lock at the time of manufacturing is shown in Figure 5A. A hard key which is paired with a lock at manufacturing is a master key (“**Master Key**”) herein.

[0146] The lock **100** comprises a main housing which is a hard and robust metal casing inside which a drive mechanism, a portion of the lock mechanism, a controller, a wireless data communication frontend, a key interface and a power management circuit are housed. The lock mechanism comprises a lock arm which is movable between a locking position and an unlocking position. The lock arm comprises a first portion which is permanently received inside the metal housing and which is pivotally movable relative to the main housing and about its axis. The first portion of the lock arm is an axial portion which is movable along an axial direction of its axis between a locking position and an unlocking position. The first portion has a first recess and is under spring urge to move along its axial direction and away from the locking position towards the unlocking position.

[0147] The second portion is an axial portion which is offset from the first portion and which is pivotally movable relative to the main housing and pivotally movable about the axis of the first portion as a pivotal axis. The second portion is also movable in a direction parallel to its pivotal axis between a locking position and an unlocking position and has a second recess. The second recess is inside the main housing when in the locking position and outside the main housing when in the unlocking position.

[0148] The lock mechanism comprises a latching member which is movable between a latching position and a releasing position.

[0149] When the lock arm is in the locking position and the latching member is in the latching position, the lock is in the locked state and the lock arm is locked at its locking position.

[0150] When the latching member is in the releasing position, the lock is moved into the unlocked state and the lock arm is moved into its unlocking position by the spring urge acting on the first portion of the lock arm.

[0151] Referring to Figures 4A-4C, the latching member comprises a pair of bullet heads **102**. The bullet heads **102** are in complementary engagement with the recesses on the lock arm **104** when the lock is in its locked state. The bullet heads are opposite end portions of a latching device and are on opposite diametric ends of the motor shaft **106**. The bullet heads project from opposite diametric sides of the motor shaft and the latching device extends in a transverse direction orthogonal to the motor axis. The transversal extent of the bullet heads, measured from free-end to free-end, is comparable to the clearance between the recesses of the lock arm.

[0152] The latching device is driven by a drive mechanism to move between a latching position and a releasing position as shown in Figures 7A and 7B respectively. The drive mechanism

comprises a motor **106** having a motor shaft which is rotatable about a motor axis and a motor driving circuit. The motor may be a brushless DC motor and the motor driving circuit may comprise a driving bridge for driving the motor.

[0153] The motor is electrically connected to the motor driving circuit which is controlled by the controller. The controller is configured to operate the drive mechanism to drive the motor to rotate the latching member between the latching position and the releasing position.

[0154] A Toshiba TC35680, which is a Bluetooth Low Energy (5) single-chip controller with built-In flash ROM, is used as an example controller. The wireless transceiver to facilitate Bluetooth (BT) data communication is on-board the controller so that no separate wireless data communication frontend is required for enhanced compactness and cost efficiency. The lock arm is configured as an antenna for wireless signal reception and transmission. The controller and the motor driving circuit are mounted on a printed circuit board ("**PCB**"). The example PCB is mounted on a side of the motor for compactness.

[0155] The example lock requires user activation in order to commence operational service for the first time after factory delivery. In example embodiments, the example lock at its ex-factory state has its User Key set to **Invalid** and its Default Key set as Admin Key. To activate the lock, a first owner of the lock is required to initialize the lock by engaging into data communication with the host server and to register ownership with the host server. In example embodiments, an owner may operate a mobile data communication apparatus such as a smart phone to capture an image of an encrypted identification code and send the captured image of the scanned encrypted identification code to the host server. The host server upon verification of the authenticity of the identification code is to send the softkeys to the user and the lock is then ready for use. The encrypted identification code may be formed by encryption of a hashed MAC address of the lock by the Default Key of the lock. After the user is in possession of the softkeys, the user may save the softkeys and the identification code of the lock on the Master Key, the Smart phone or other data communication apparatus ("**APP**") for subsequent use. A plurality of User Keys of a plurality of locks may be stored on a single data communication apparatus and the user may execute stored instructions to operate the lock. A lock may be assigned a nickname by a user for ease of recognition and use. A nickname can be for example, garage door, bicycle 1, etc. without loss of generality. The APP may have lock information including identification code and or nickname of the locks, their respective softkeys and their respective statuses arranged in the form of a lock table.

[0156] The softkeys saved on the APP may include User-Keys and/or Admin-Keys. For example, a user may be granted right to open and/or close a lock in which case the user is only given a copy of the User-key, but not a copy of the Admin-Key. Where the APP is a Master Key paired with, say lock 1 (Garage), the APP will have both UserKey and AdminKey. Likewise, an APP may be an administrator given with administration right only, in which case the APP of the administrator may be given a copy of the AdminKey only (and not the UseKey). The status “Registered” means the hardware identification of the hard key has been registered with the specific lock and “Unregistered” means the hardware identification of the hard key has not be registered with the specific lock.

[0157] In example operations, the user is to activate the dedicated application software (App) on the data communication apparatus **300** to operate the lock. The data communication apparatus on executing the App will become an APP (or hard key) which is operable to transmit the softkeys to operate the lock. Initially, the APP will commence wireless scanning to make inquiries to locate the lock. The lock in response will transmit its identification code, which in this example is its MAC address, by wireless data communication in Bluetooth LE (“**BTLE**”) protocol. The APP upon receipt of the identification code via BTLE transmission will look up its storage and determine whether the lock is one which is operable by the stored softkeys and to pair with the lock. The APP can then operate the lock using the App and the commands of the App.

[0158] In example operations, a user may operate the lock with the Master Key in physical contact with the lock.

[0159] Referring to Figure 4B, the example lock has a USB port **108** on its main housing and the Master Key has a compatible and complementary USB portion on its main housing such that the USB port on the lock and the counterpart USB port on the Master Key can enter into mated engagement. In this example, the key interface port of the lock has the form and configuration of a USB Micro-B female connector and the lock interface port of the Key has the form and configuration of a USB Micro-B male connector which can enter into mated physical engagement with the key interface of the lock.

[0160] The example lock interface port **202** of the key **200** comprises an example plurality of 5 key interface terminals (or pins) and the pins have same description as the terminals of the USB connector herein.

[0161] The example lock is configured to monitor status at the identification terminal of the key interface. When the status at the identification terminal signifies that a hard key compatible with

the lock is present, the lock is to commence data communication and data communication will take place through the data communication terminals, namely terminals 2 and 3.

[0162] In example embodiments, a signature identification voltage present at the identification terminal will wake up the lock. When the lock is woken up by the signature identification voltage, the lock will proceed to commence data communications through the key interface terminals.

[0163] In example embodiments such as the present, data communications which are to take place through the key interface are wired data transmission, for example, in serial form by means of a serial port protocol.

[0164] In example embodiments, the data exchange which is to take place through the key interface is confined to non-secured data such as device identification data, for example, the MAC address or the serial number of the lock and the hard key.

[0165] When identification data of the lock are received by the hard key, the hard key will look up its lock table and determine whether the lock is an eligible lock for the hard key. An eligible lock is one that is on the lock table of the hard key.

[0166] If the lock is on the lock table of the hard key, which means that the lock is ready to be operable by the hard key, the hard key will switch to wireless data communication with the lock. In example embodiments such as the present, the wireless data communication is facilitated using BTLE protocols since both the lock and the hard key is Bluetooth enabled. In some embodiments, the lock and the hard key may be configured to facilitate data communication using other wireless data communication protocols without loss of generality. If the lock is not on the lock table, the hard key will turn off its power output to preserve power.

[0167] After the lock has sent out its device identification data, the lock is to switch into a discoverable mode to be discoverable and the hard key is to perform scanning and search for a matched Bluetooth device having the device identification data for Bluetooth pairing. Once the lock is found by the hard key, the hard key will initiate a connection request, for example, via standard Bluetooth "Just-Works" model to establish Bluetooth data connection.

[0168] After the lock and the hard key have established wireless data connection, the hard key will look up its lock table to check whether the hard key has operated the lock before. If the hard key had operated the lock before, the lock would have a "Registered" status assigned on the lock table. Otherwise, the lock would not have a "Registered" status and may have, for example, a "Not-Yet-Registered" status. If the lock does not have a status of "Registered", signifying that the hard key has not previously operated, for example, open or close, the lock, the hard key is to send

an instruction to request the lock to add or include the hard key as an eligible hard key, and the instruction may include the device identification data of the hard key. The instruction may have a command name of "Add_Master-Key".

[0169] After the lock has received and accepted the "Add_Master-Key" command, the hard key #6 having the example MAC address is admitted as an eligible hard key for operation of the lock, and the lock will update its key table.

[0170] After the acceptance and table update have been complete, the newly admitted hard key will be entered on the key table of the lock and assigned a "Valid" status, and the lock will send an acknowledge to the hard key. A "Valid" status means the hard key has passed the admittance procedure to be operable. When the hard key is on the key table and assigned a "Valid" status, the admitted hard key may create and send operational commands to the lock, for example, the Lock_Open command to open the lock.

[0171] On the other hand, if the lock is on the lock table and has a "Registered" status, this means the hard key had previously registered with the lock and the lock has a record of the identification code of the hard key on its key table, the lock will communicate with the hard key and take operational commands from the hard key, subject to authenticity check of the operational commands.

[0172] In some embodiments, the hard key may be configured to verify its status with the lock even though the lock is on the lock table and has a "Registered" status, since the "Registered" status may have become obsolete due to intervening events, such as intervening registration of a new owner or intervening disabling of the hard key.

[0173] In example embodiments, the hard key may be configured to send a command to request for a verification of its status vis-a-vis the lock. The command may have code-named **"Key_valid_Check_Request"**.

[0174] In response, the lock will send a Key_valid_Check_Response.

[0175] If the return value of the Key_valid_Check_Response signifies that the hard key is valid, the hard key may send an operational command such as a Lock_Open_Request to open the lock.

[0176] Upon receipt of a command such as an encrypted Lock_Open_Request message, the lock is to decrypt the message using the UserKey of the hard key which sends the command to extract the embedded command. If the decryption is successful, the lock shall proceed to perform the operation stipulated by the command.

[0177] In example embodiments, the controller of the lock is configured to switch the operation power supply of the lock from the built-in power source to the hard key. In such embodiments, the controller comprises a power switching circuit. The power switching circuit may be controlled by the controller or a built-in power control circuit.

[0178] For example, when a signature voltage signifying the insertion of a hard key is detected at the key interface of the lock, the controller or the power switching circuit will recognize the signature voltage as an identification signal of a hard key and operate to change power supply so that the operation power of the lock is provided by the hard key, instead of the internal power supply of the lock to preserve power of the lock to extends its time before charging. An example hard key may have buttons pre-set on the main housing for operating the lock. The preset buttons may include a “lock” button, an “unlock” button, and/or other functional buttons without loss of generality. A button herein may be a mechanical button or an electronic button such as a sensing tab on a panel.

[0179] A hard key may operate a lock remotely, that is, without physical contact between the lock and the hard key, for example using BTLE protocol. For example, a Mastery Key may operate its default lock remotely without having the lock interface and the key interface in mated engagement. In example embodiments, a Master Key may have a default button or default buttons assigned for remote operation of the default lock. A default lock (“Default Lock”) herein is a lock which is paired with the Master Key at the time of manufacturing or at the time of delivery. For example, if there is only one lock which is stored or registered on the hard key and/or is in an activated or valid status, the key controller on detection of operation signal at the preset button will commence wireless data communication with the controller of that lock and to perform operations according to the command instructions. For example, when the Default Lock is the only lock which is stored or registered on the Master Key, pressing a preset button on the Master Key will lead to operation of the Default Lock. In example embodiments, the controller upon detection of operation signal of a preset button will determine whether there is only one operable lock stored on the hard key and to proceed to operation of the operable lock if it is determined that there is only one operable lock.

[0180] The softkeys and hard keys which are in force may be updated from time to time remotely.

[0181] For example, if a hard key is reported loss, the APP may execute stored instructions such as a remove key or disable key command and the lock upon receipt of the instructions will remove or disable the keys.

[0182] Alternatively, or in addition, the APP may execute stored instructions to change the UserKey and the AdminKey and notify the lock to update the changes. As a result, obsolete keys having obsolete UserKey and AdminKey will no longer pass the decryption procedure.

[0183] In example embodiments, the authentication of device identification data is implemented via contactless method, for example, near field communication (NFC). Referring to Figure 11, the example electronic lock is a NFC tag and the example electronic key is a NFC reader. The NFC tag is a passive device, which means that it operates without a power supply of its own in the authentication stage. It enters into sleep mode if no activity is detected for a predetermined period of time, thereby power is preserved. Connectivity and authentication is initiated when the key is placed in proximity to the lock.

[0184] While the present disclosure has been made with reference to example and embodiments, the example and embodiments are non-limiting and are not intended to limit the scope of disclosure.

[0185] For example, the lock may be implemented as a lock of a smart safe box, a door lock or in other forms as shown in Figures 12A – 15B. The terms UserKey and User Key are used interchangeably and the terms AdminKey and Admin Key are used interchangeably.

Claims

1. A lock comprising a controller, a data storage device, a lock mechanism operable by the controller in a locked state or an unlocked state, and a data communication frontend comprising a first data port and a second data port;

wherein the controller is configured to enter into data communication via the second data port after successful completion of data communication via the first data port.

2. The lock according to claim 1, wherein the controller is configured to receive identification data via the first data port and to receive operational data messages via the second data port, and wherein the controller is configured to not to receive operational data messages via the second data port if the identification data received via the first data portion does not meet an admission criterion.

3. The lock according to claims 1 or 2, wherein the controller is configured to conduct unencrypted data communication via the first data port and encrypted data communication via the second data port.

4. The lock according to any preceding claims, wherein the first data port is a data port configured for wired data communication or wireless data communication and the second data port is a data port configured for wireless data communication.

5. The lock according to any preceding claims, wherein the first data port is configured for wireless data communication at a first modulation frequency or baseband binary data communication and the second data port is configured for wireless data communication at a second modulation frequency.

6. The lock according to any preceding claims, wherein the first data port is configured for near-field data communication and the second data port is configured for non-near-field data communication.

7. The lock according to any preceding claims, wherein a code is prestored in the lock and the controller is configured to respond by transmitting the code upon detection of the code coming in from the first data port.

8. The lock according to claim 7, wherein the code comprises a unique identification code of the lock and the controller is configured to respond by transmitting the code via the first data port.

9. The lock according to any preceding claims, wherein a first encryption key which is built-in encryption key is permanently stored on the lock and the controller is configured to use a second encryption key to retrieve lock operation instructions include locking and unlocking instructions, and wherein the controller is configured to retrieve the second encryption key using the built-in encryption key.
10. The lock according to claim 9, wherein the second encryption key is embedded in a data message received via the second data port, and the data message is encrypted using the built-in encryption key which is a default encryption key.
11. The lock according to any preceding claims, wherein the lock comprises a third port and the controller is configured to detect and measure a compatibility signal at the third port, and wherein the controller is configured to commence data communication via the first data port if the compatibility signal meets an admission criterion which is a first admission criterion, and not to engage in data communication via the first data port if the compatibility signal at the third port does not meet the first admission criterion.
12. The lock according to claim 11, wherein the compatibility signal is a DC signal having a DC voltage, and the controller is configured to proceed to engage in data communication via the first data port if the DC voltage at the third port is at a specific voltage level or within a specific voltage range; and/or wherein the controller is configured to proceed to engage in data communication via the first data port if the DC voltage at the third port is above the specific voltage level or not within the specific voltage range.
13. The lock according to claims 11 or 12, wherein the controller is configured to cease data communication via the first data port and/or the second data port when the compatibility signal ceases to meet the first admission criterion.
14. The lock according to any of claims 11 to 13, wherein the lock comprises a key interface for mated reception of a physical key, and wherein the key interface comprises the first data port and the third data port.
15. The lock according to claim 14, wherein the lock comprises a power management arrangement and the controller is configured to operate the power management arrangement to switch to receive lock mechanism operation power from the physical key when the physical key is physical and electrical connection with the key interface.

16. The lock according to any preceding claims, wherein the controller is configured to perform wired data communication via the first data port to determine admissibility and to switch to wireless data communication via the second data port if positive admissibility is determined during the wired data communication.

17. An electronic key comprising a key controller, a data storage device, a power source and a data communication frontend comprising a first data port and a second data port; wherein the electronic key is a physical key having a key body and is configured to work with the lock of any preceding claims.

18. The electronic key of claim 17, wherein the key controller is configured to send identification data via the first data port and to transmit operational data messages via the second data port after a positive response indicating admissibility is received via the first data port.

19. The electronic key according to any preceding claim, wherein the key controller is configured to conduct unencrypted data communication via the first data port and encrypted data communication via the second data port.

20. The electronic key according to any preceding claim, wherein a first encryption key which is built-in encryption key is permanently stored on the key and the key controller is configured to use a second encryption key to encrypt lock operation instructions before a lock operation instruction is sent to the lock.

21. The electronic key according to claim 20, wherein the second encryption key is received via the second data port in the form of an encrypted message and the key controller is configured to retrieve the second encryption key using the built-in encryption key.

22. The electronic key according to any preceding claim, wherein the key comprises a lock interface which is configured for making mated connection with a key interface of the lock, wherein the key interface comprises the first data port and a third data port, and wherein the third port is set at a DC voltage as a compatibility signal.

100

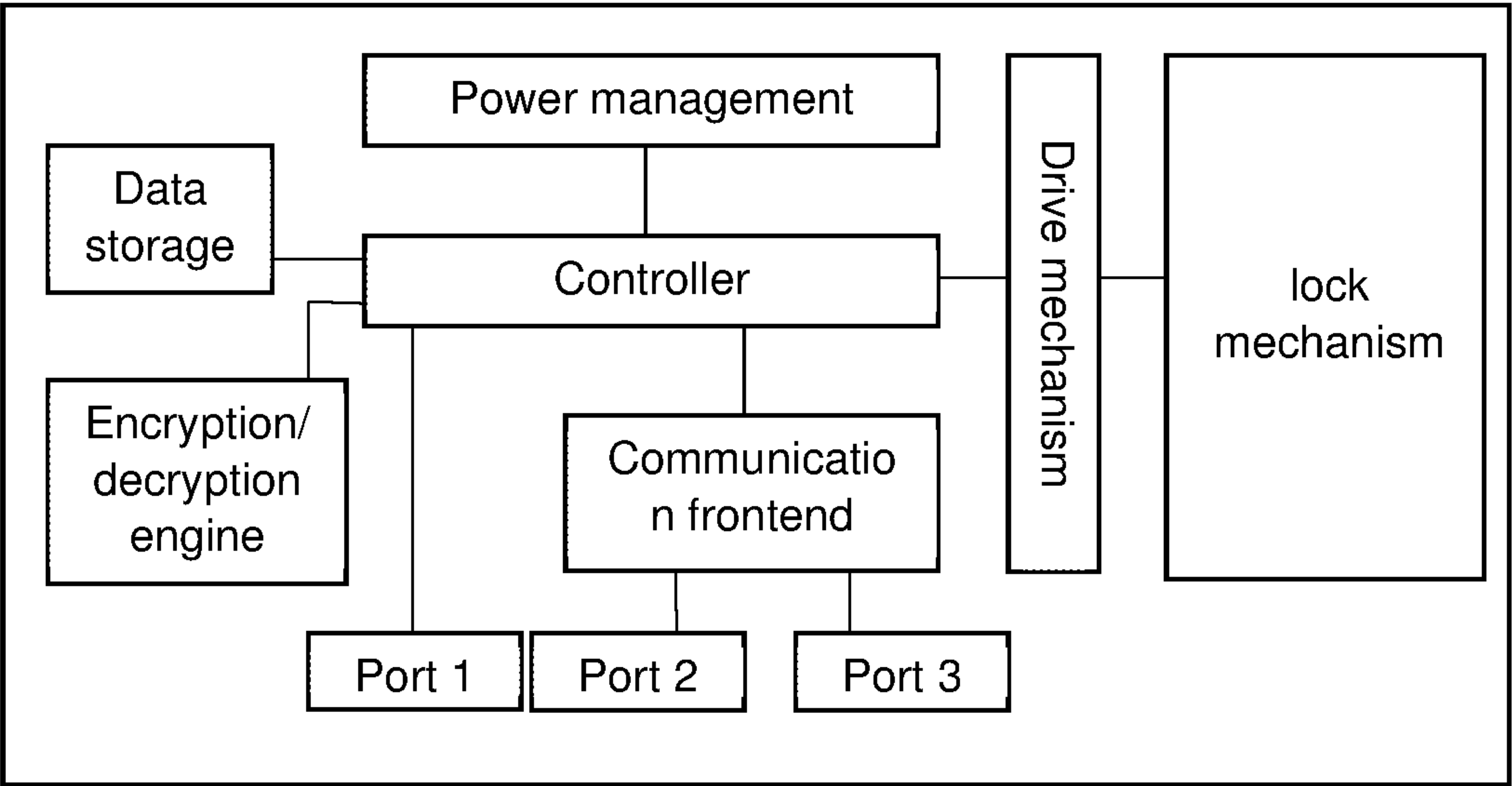


Fig. 1

100

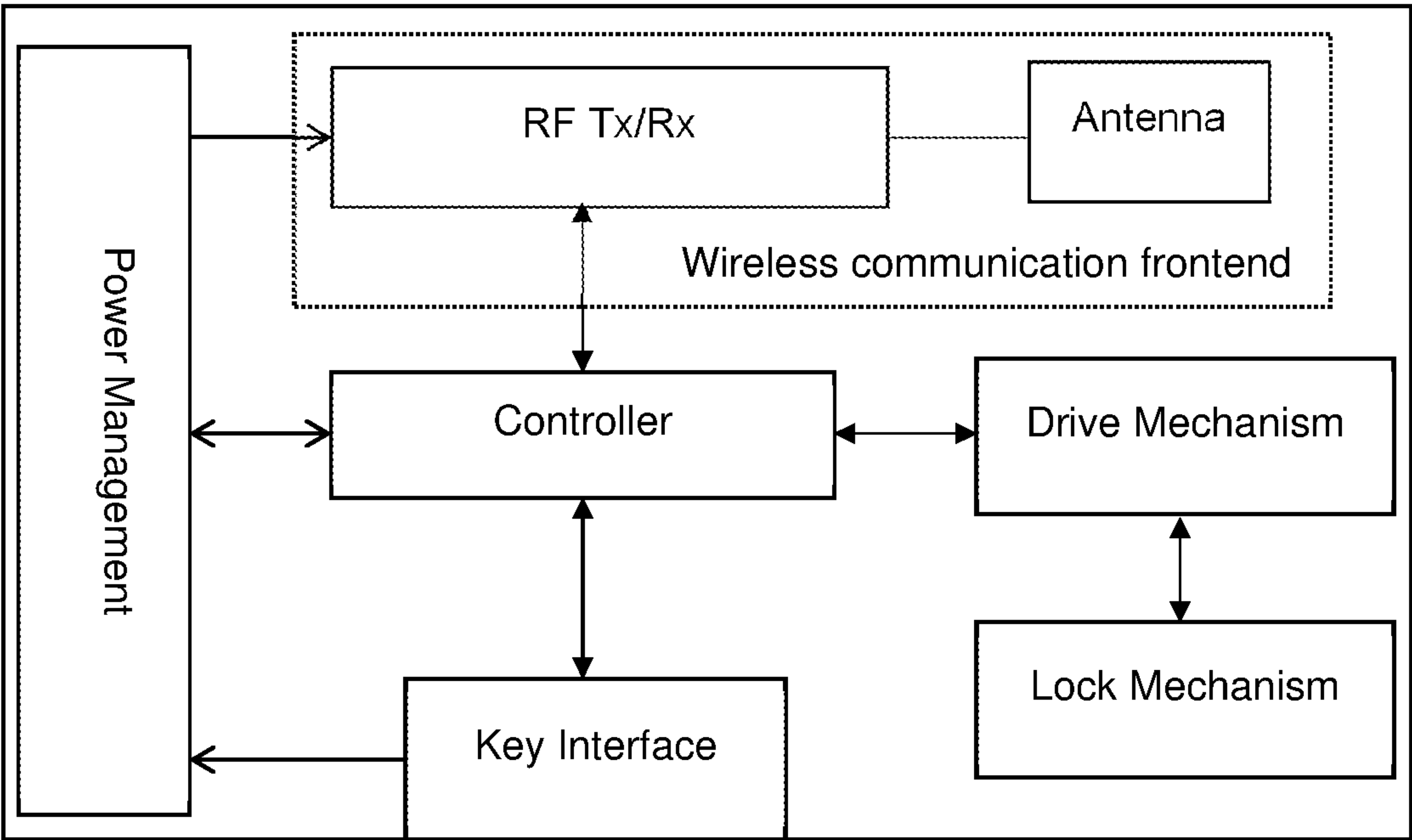


Fig. 1A

200

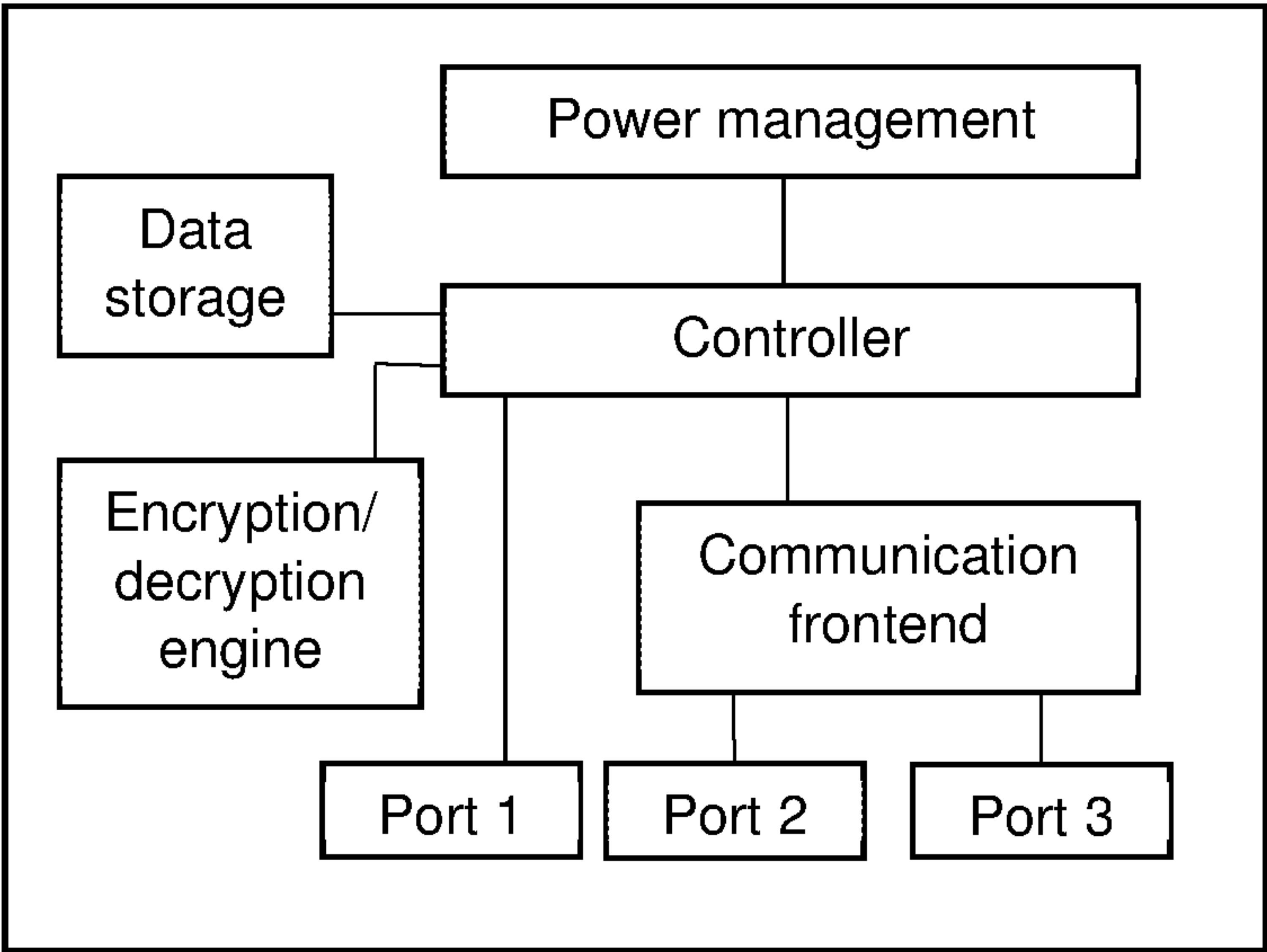


Fig. 2A

200

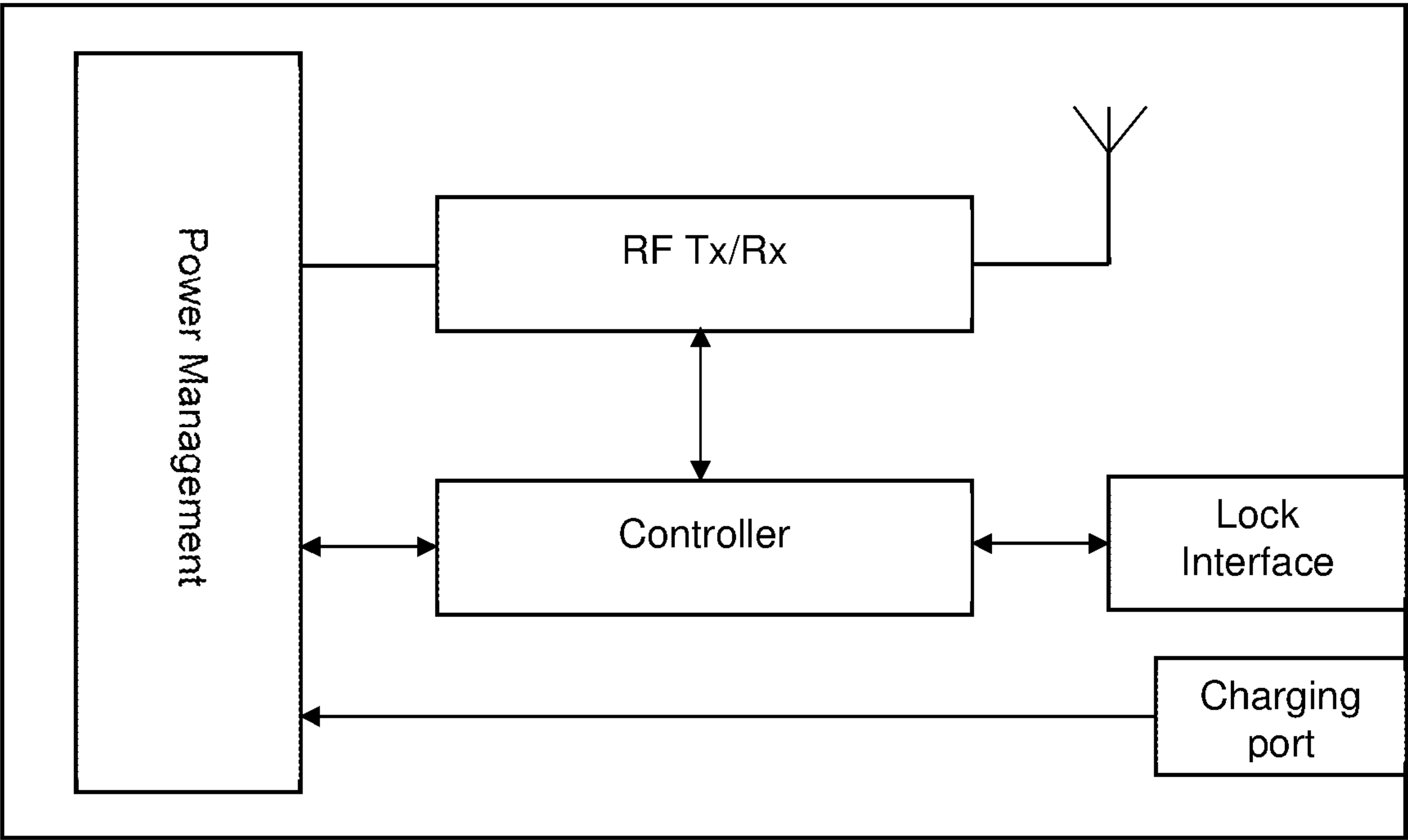


Fig. 2B

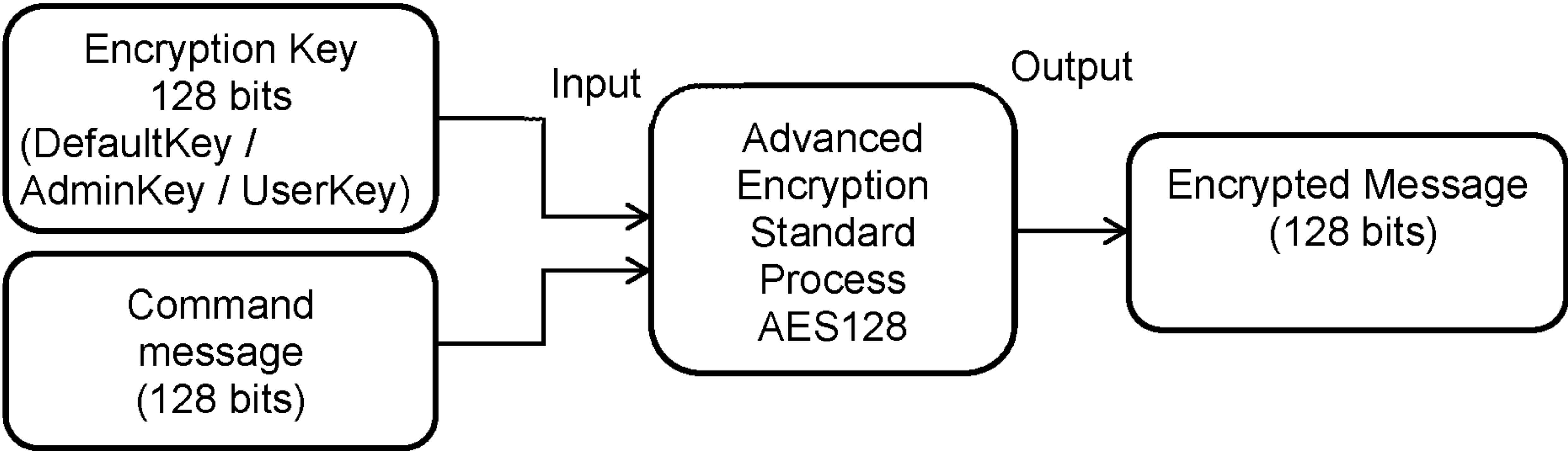


Fig. 3

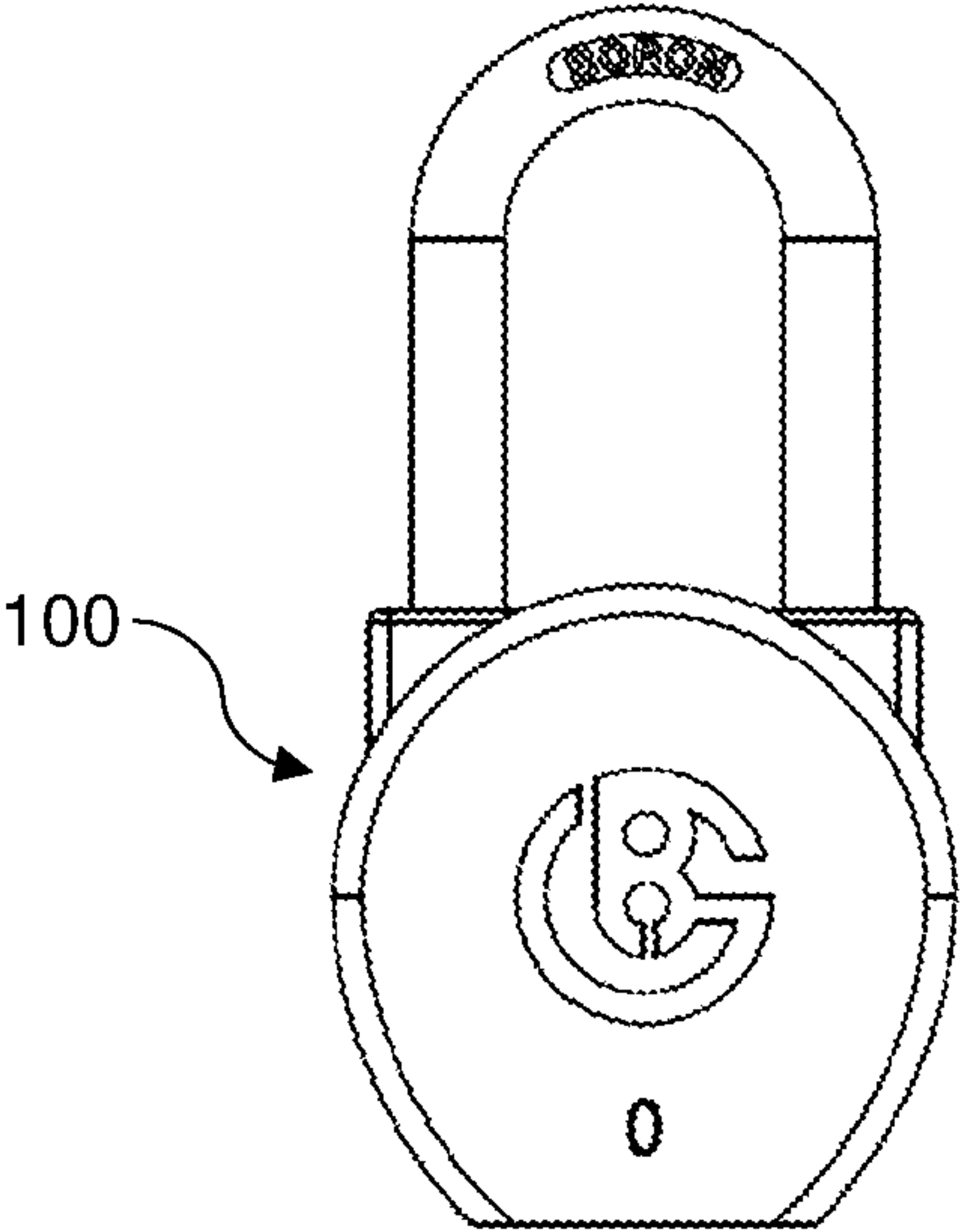


Fig. 4A

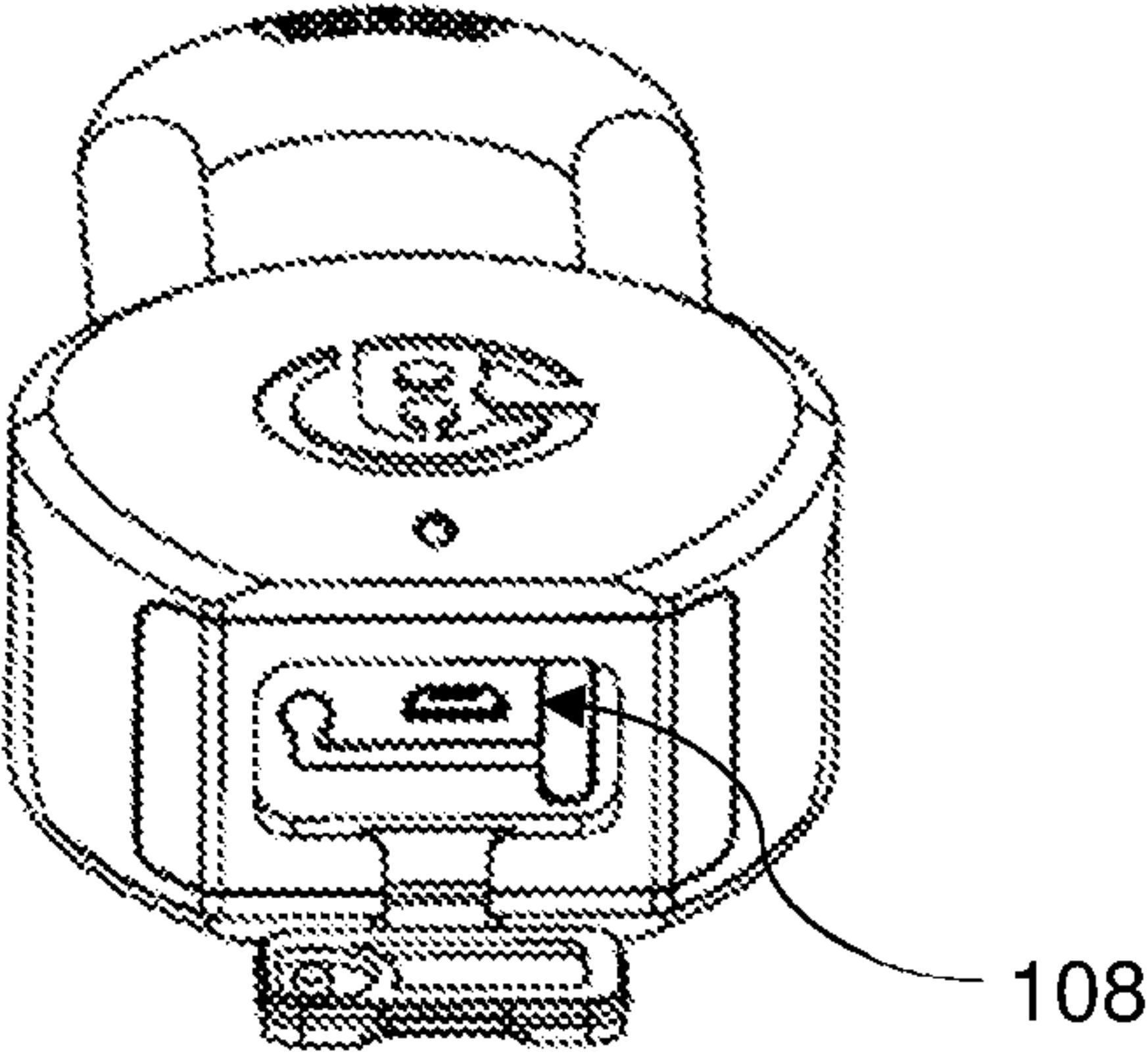


Fig. 4B

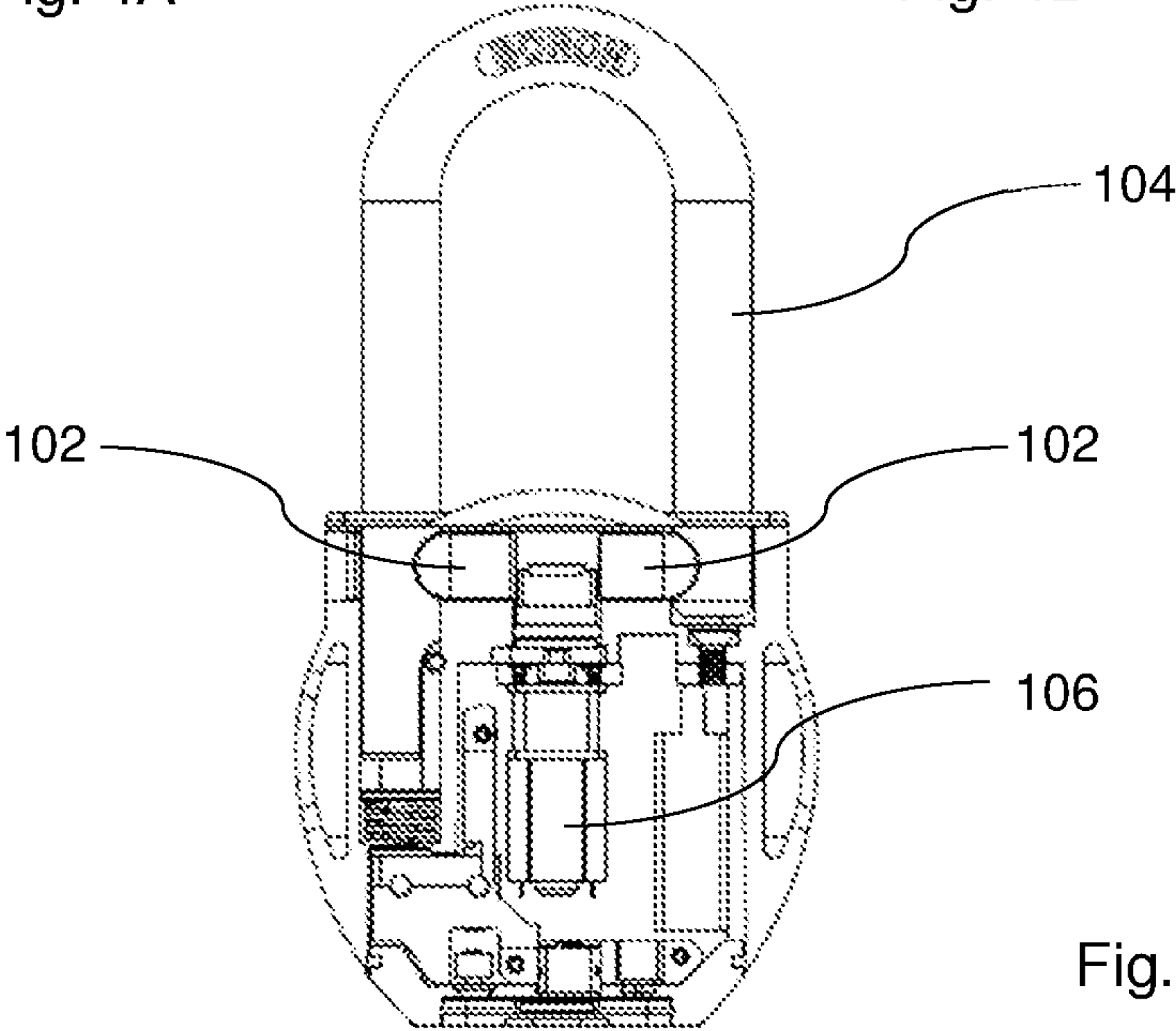


Fig. 4C

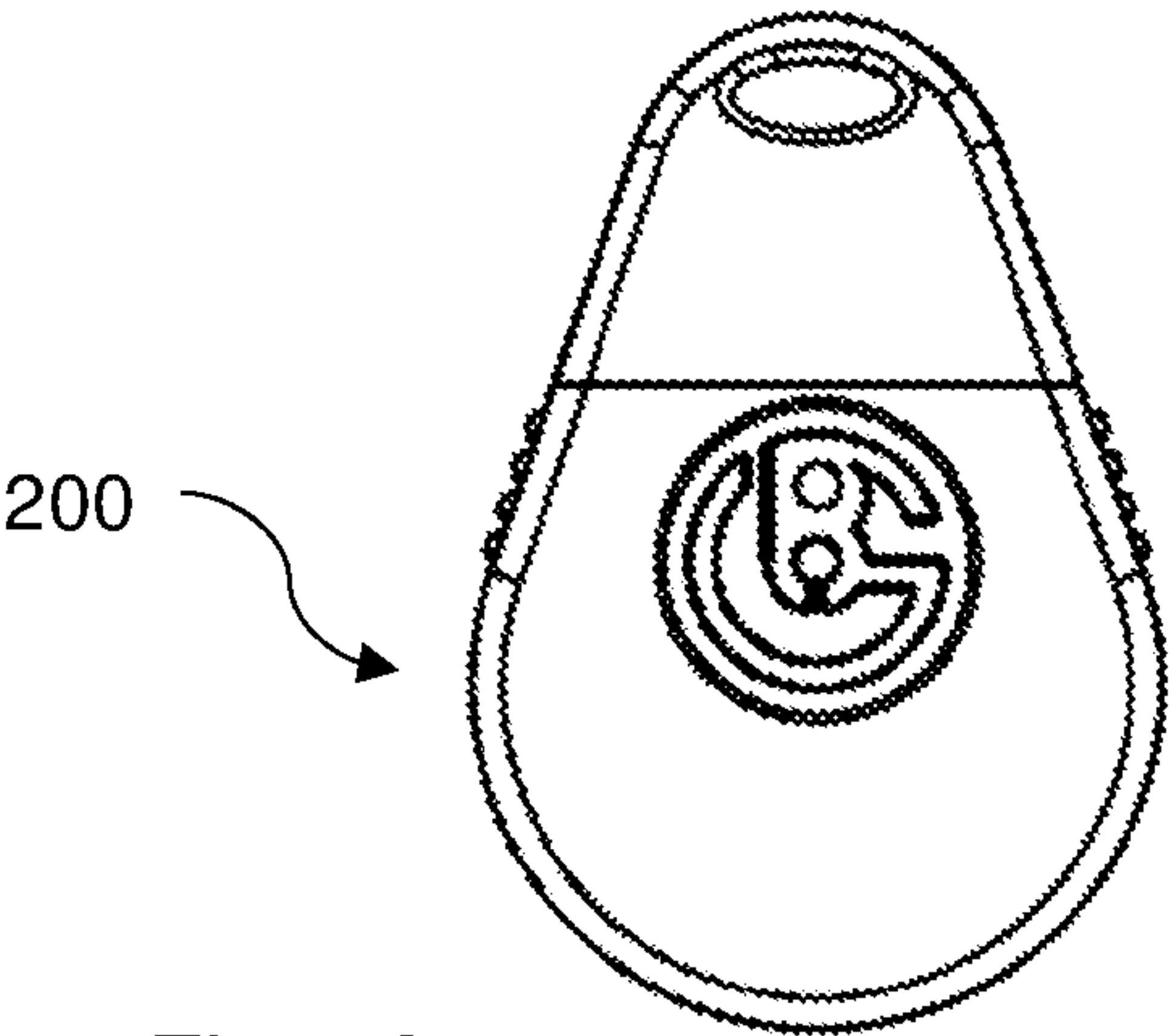


Fig. 5A

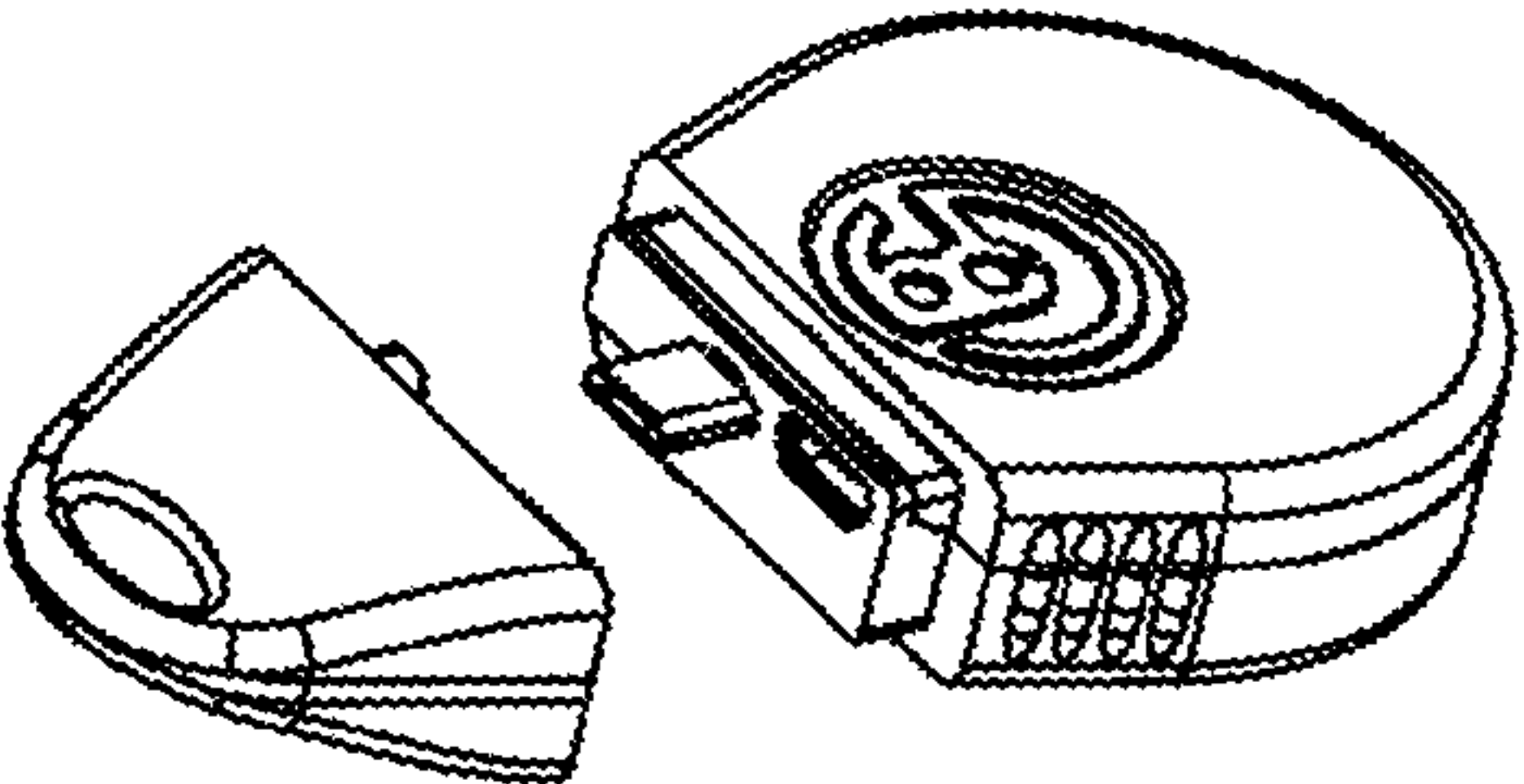


Fig. 5B

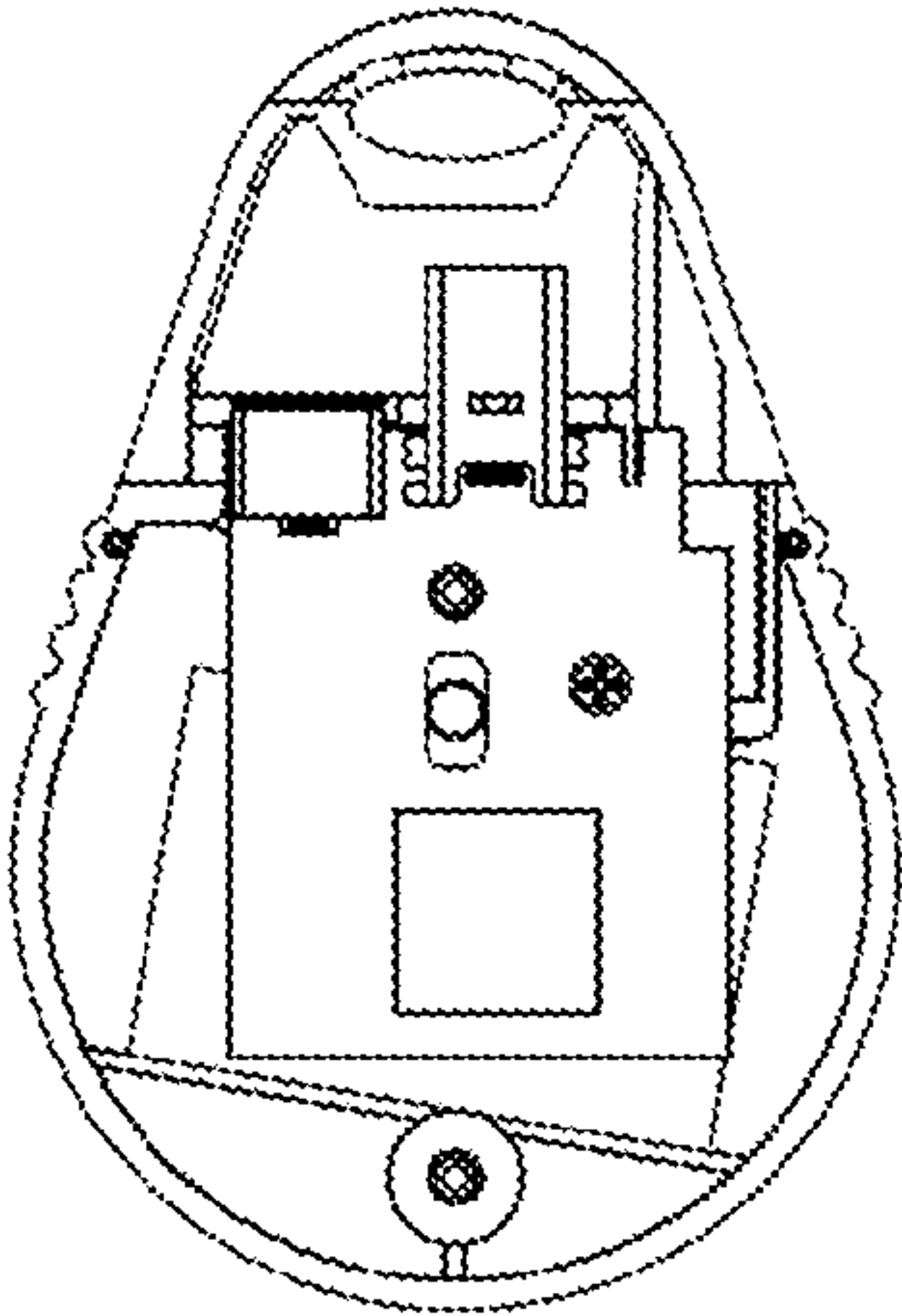


Fig. 5C

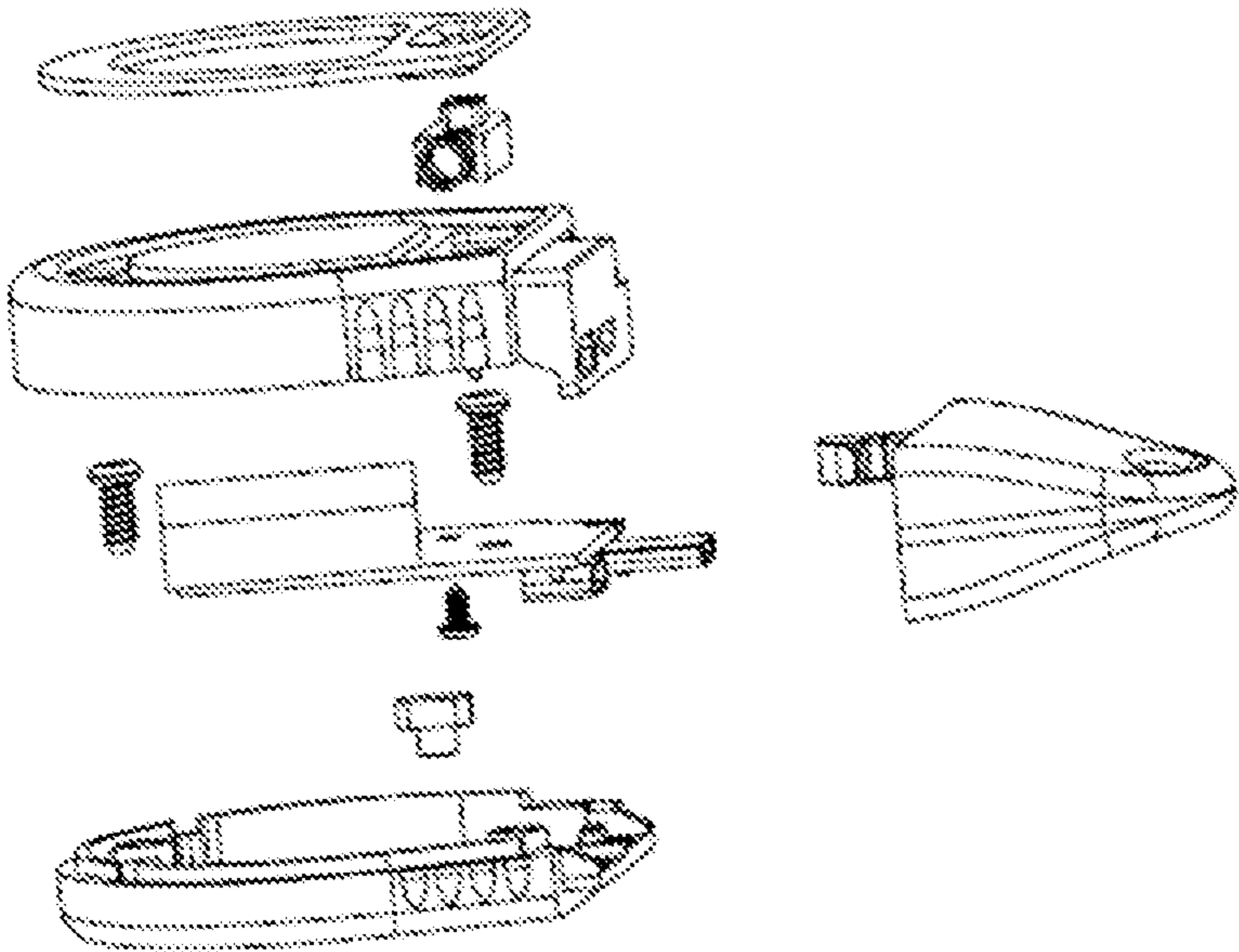


Fig. 5D

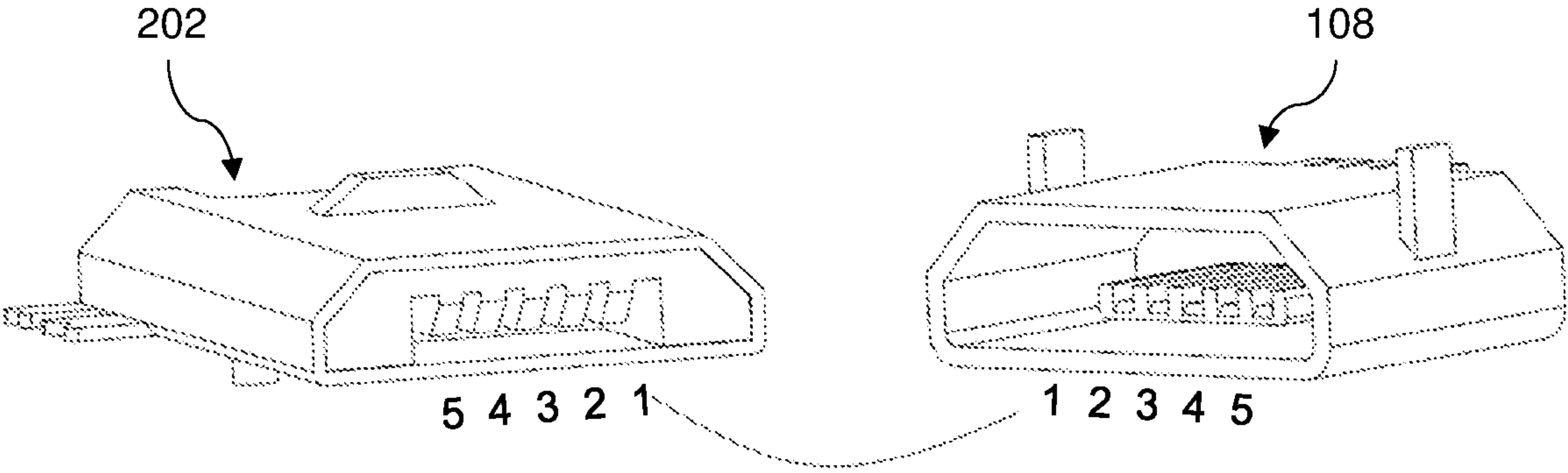


Fig. 6

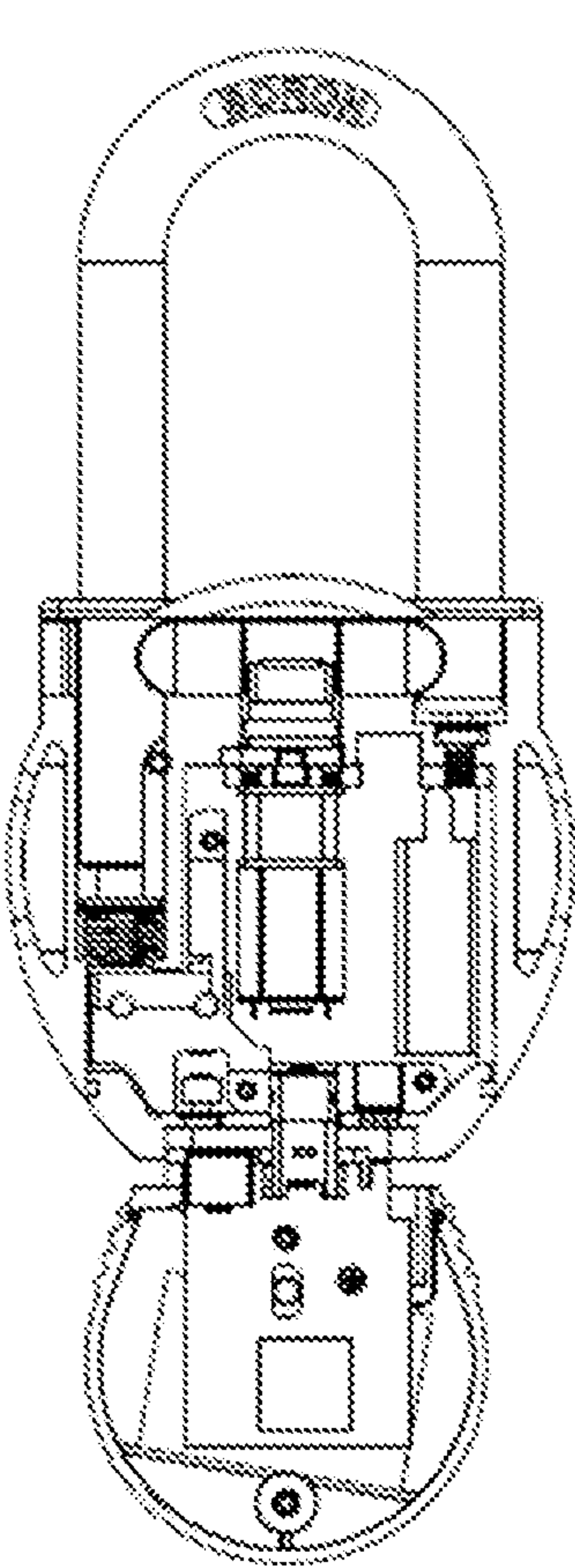


Fig. 7A

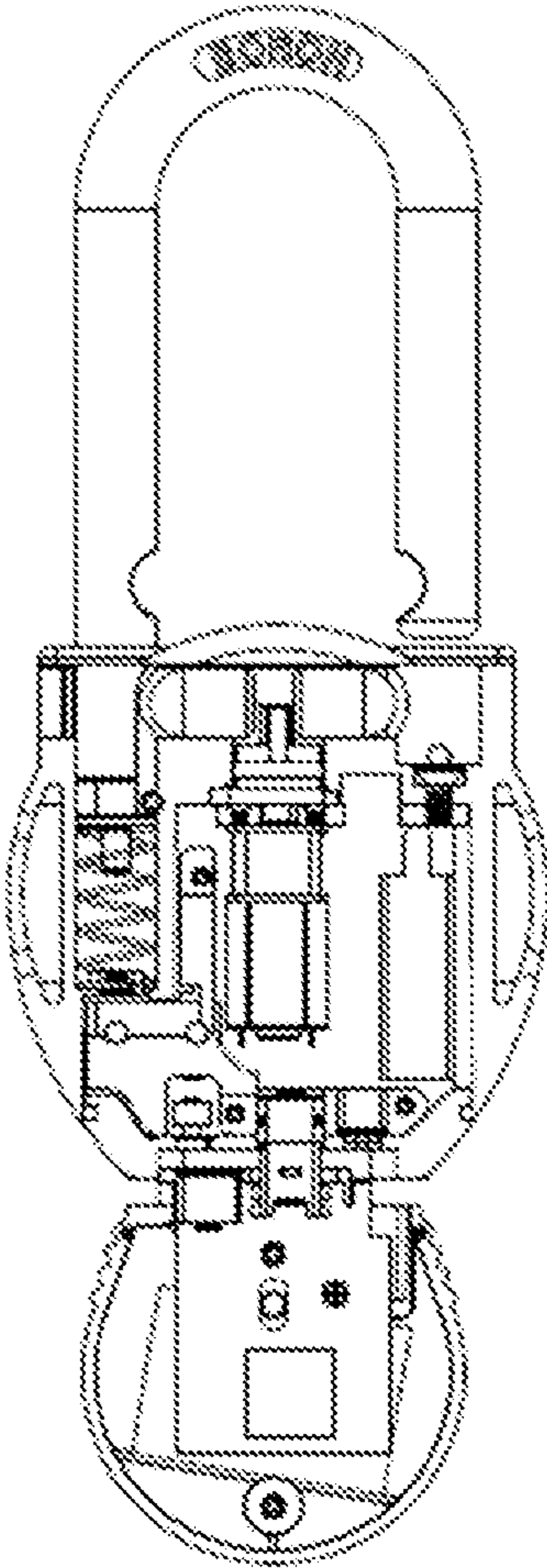


Fig. 7B

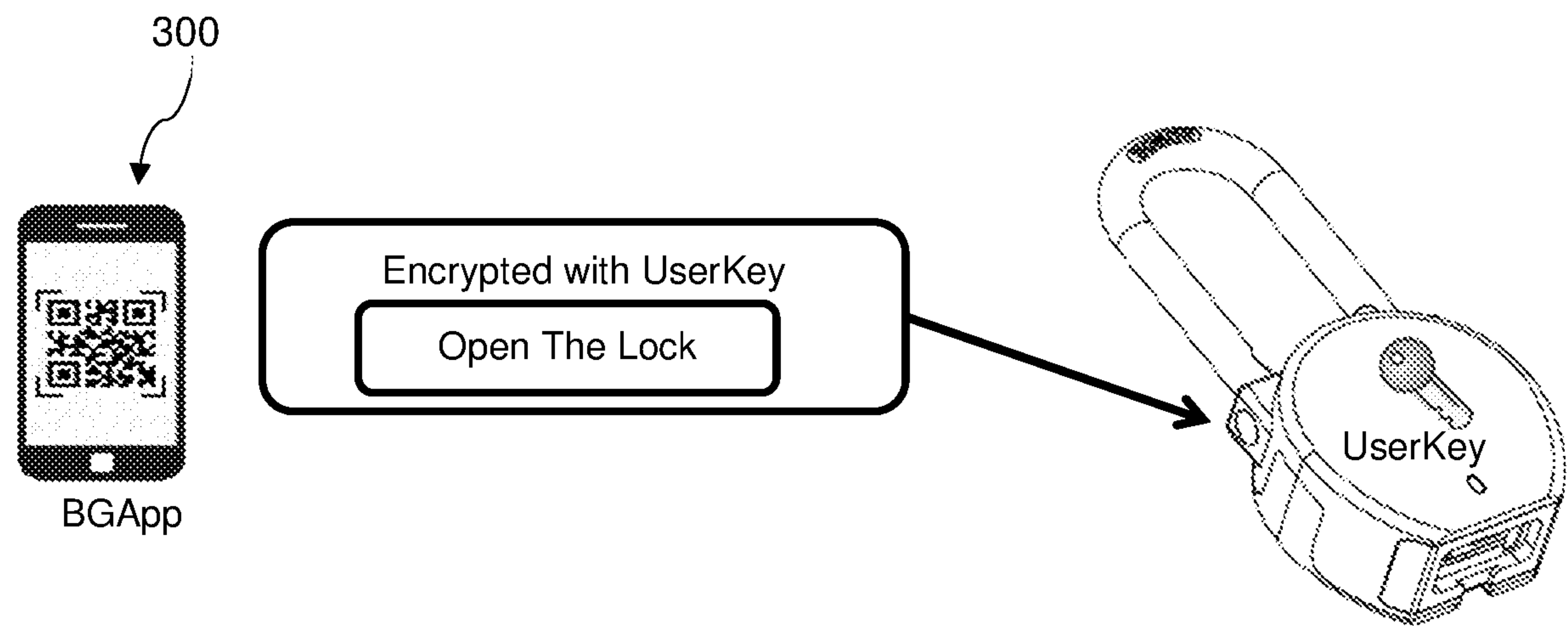


Fig. 8

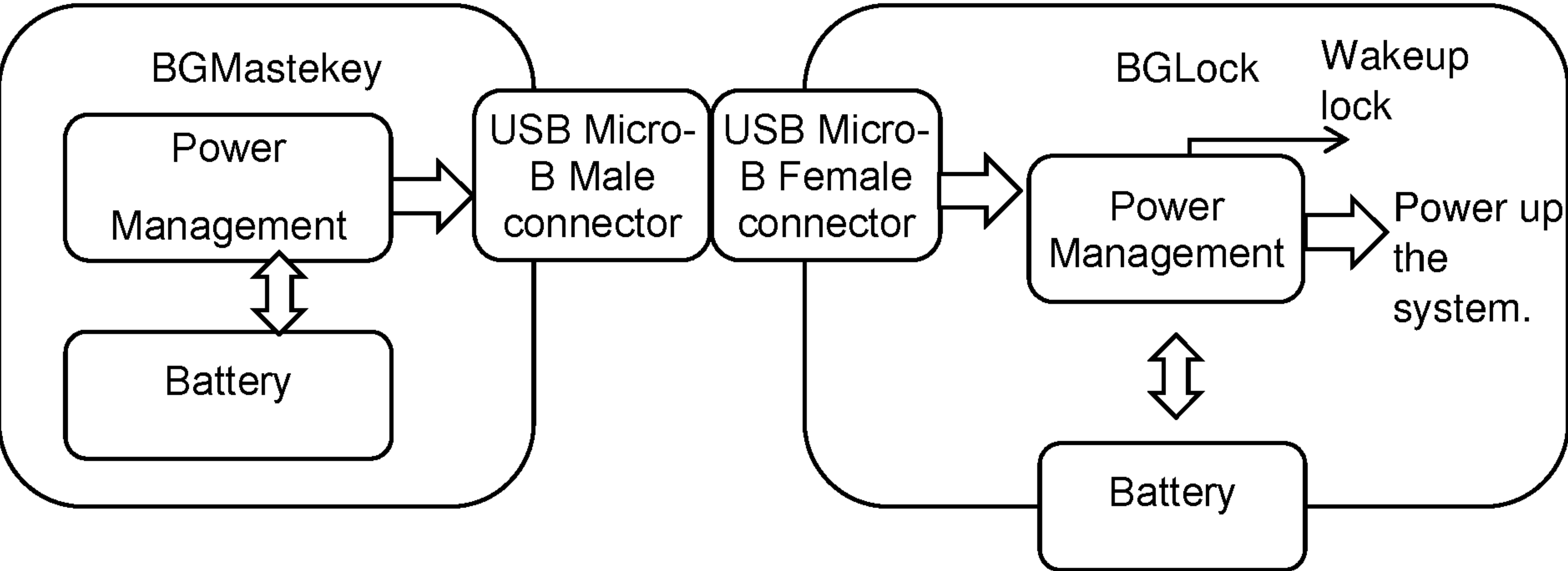


Fig. 9

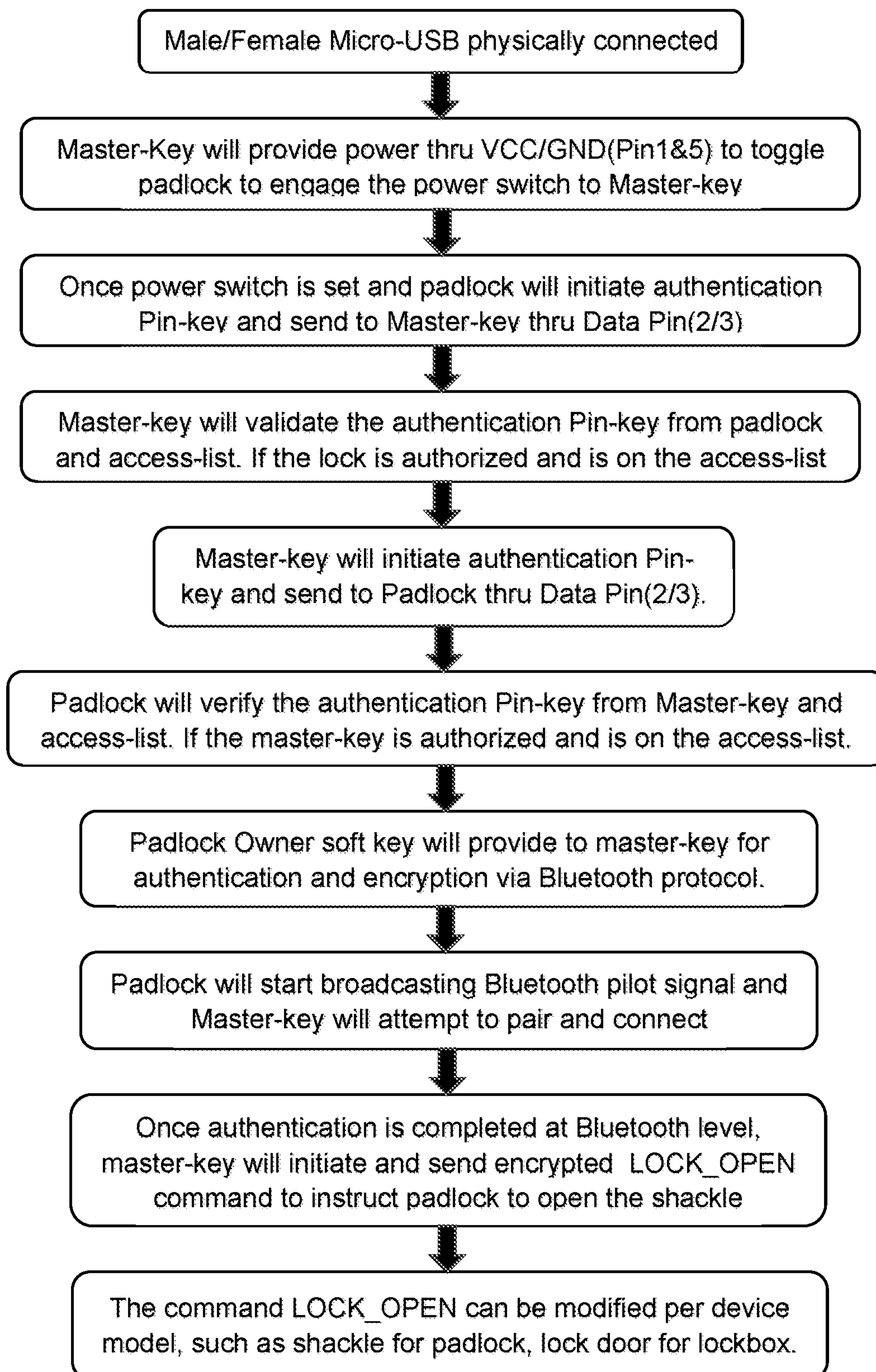


Fig. 10

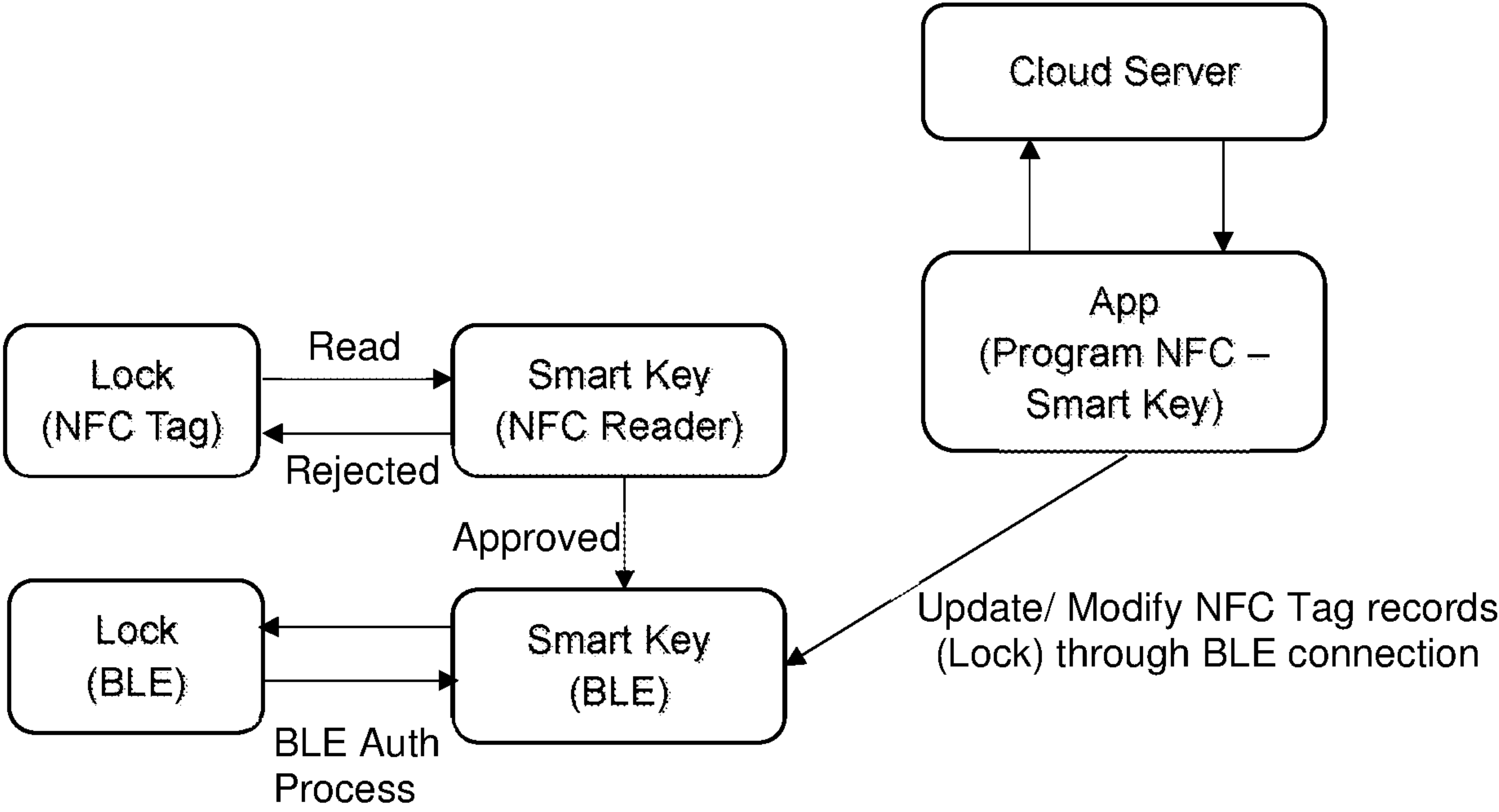


Fig. 11

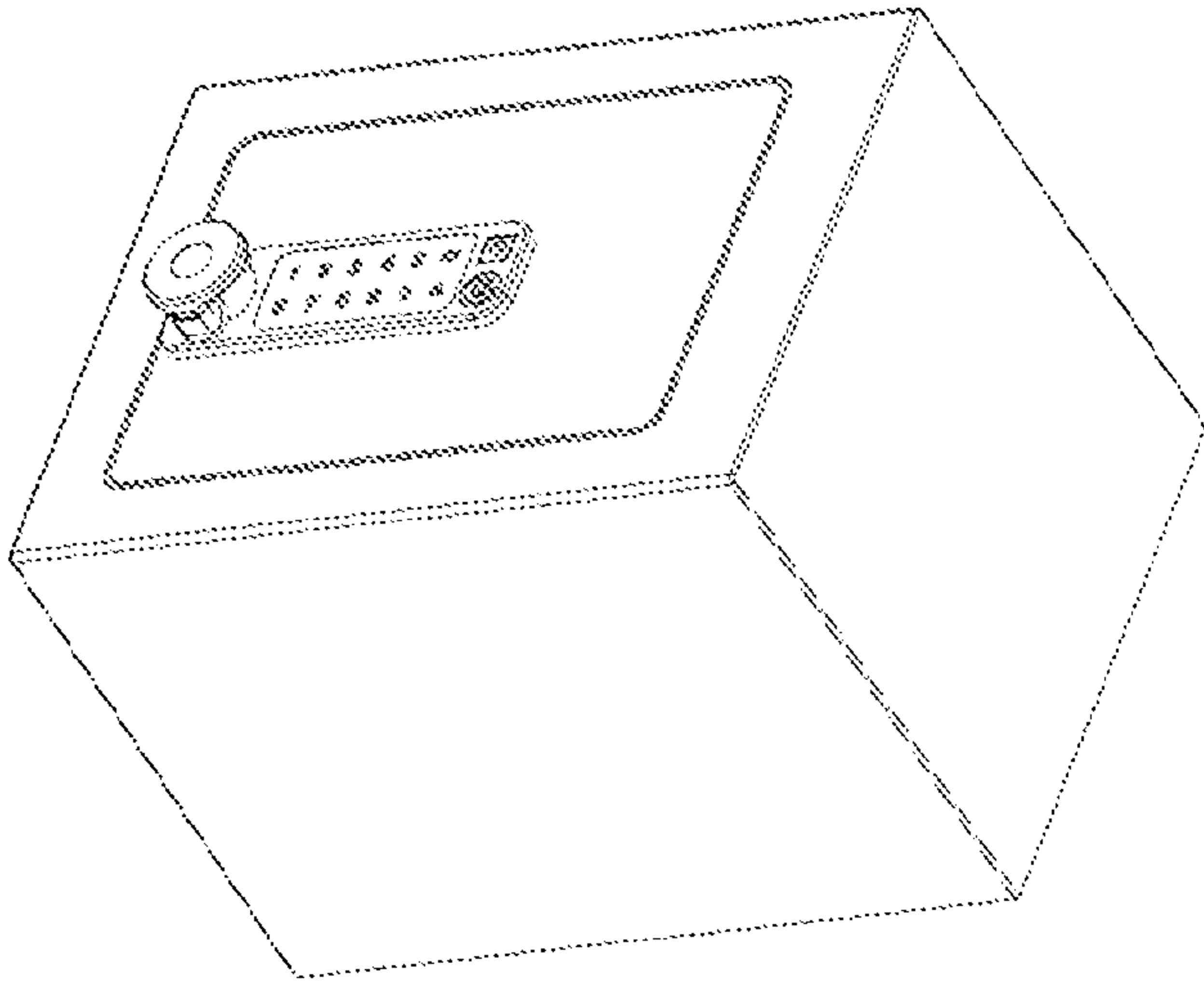


Fig. 12A

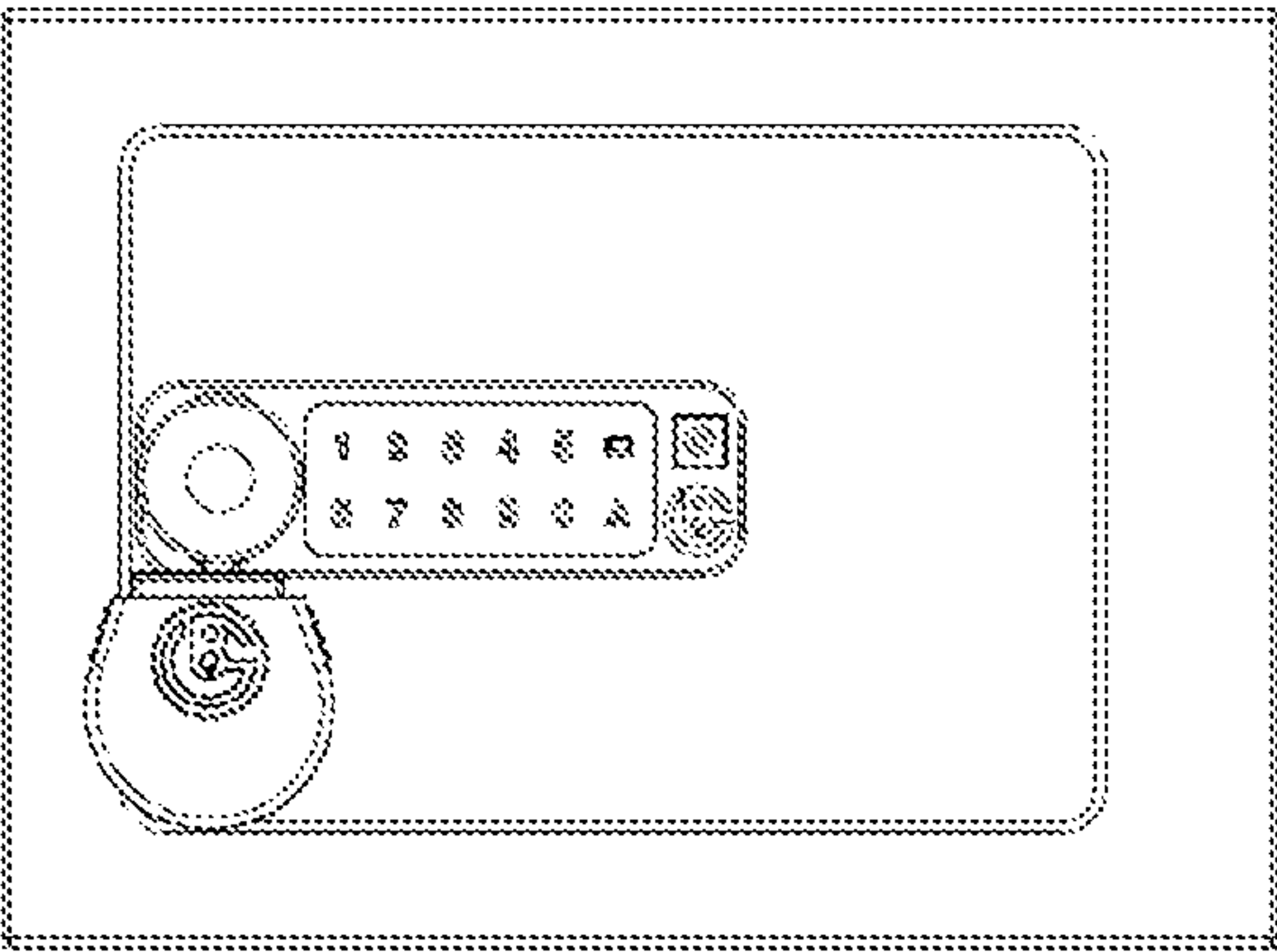


Fig. 12B

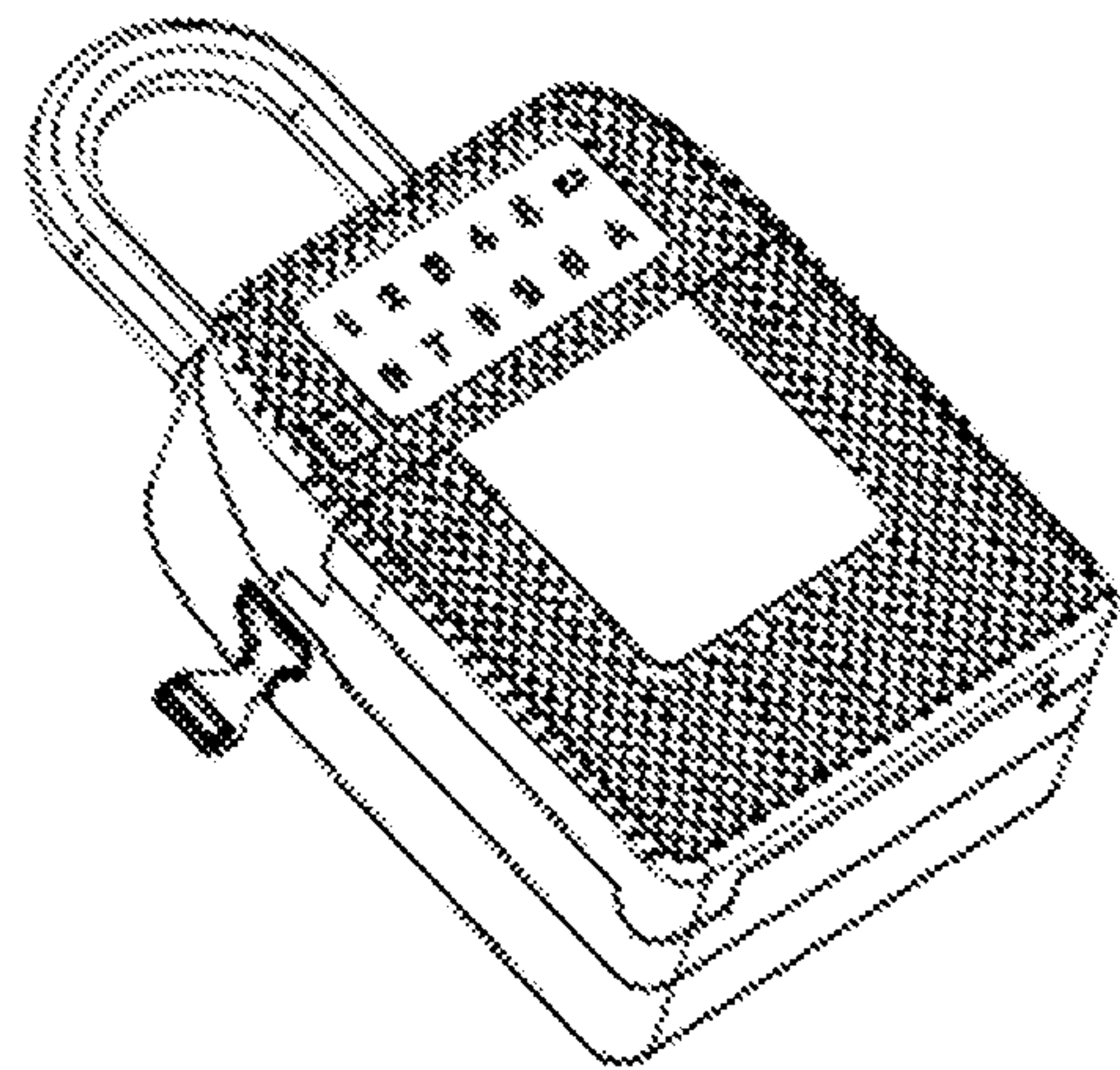


Fig. 13A

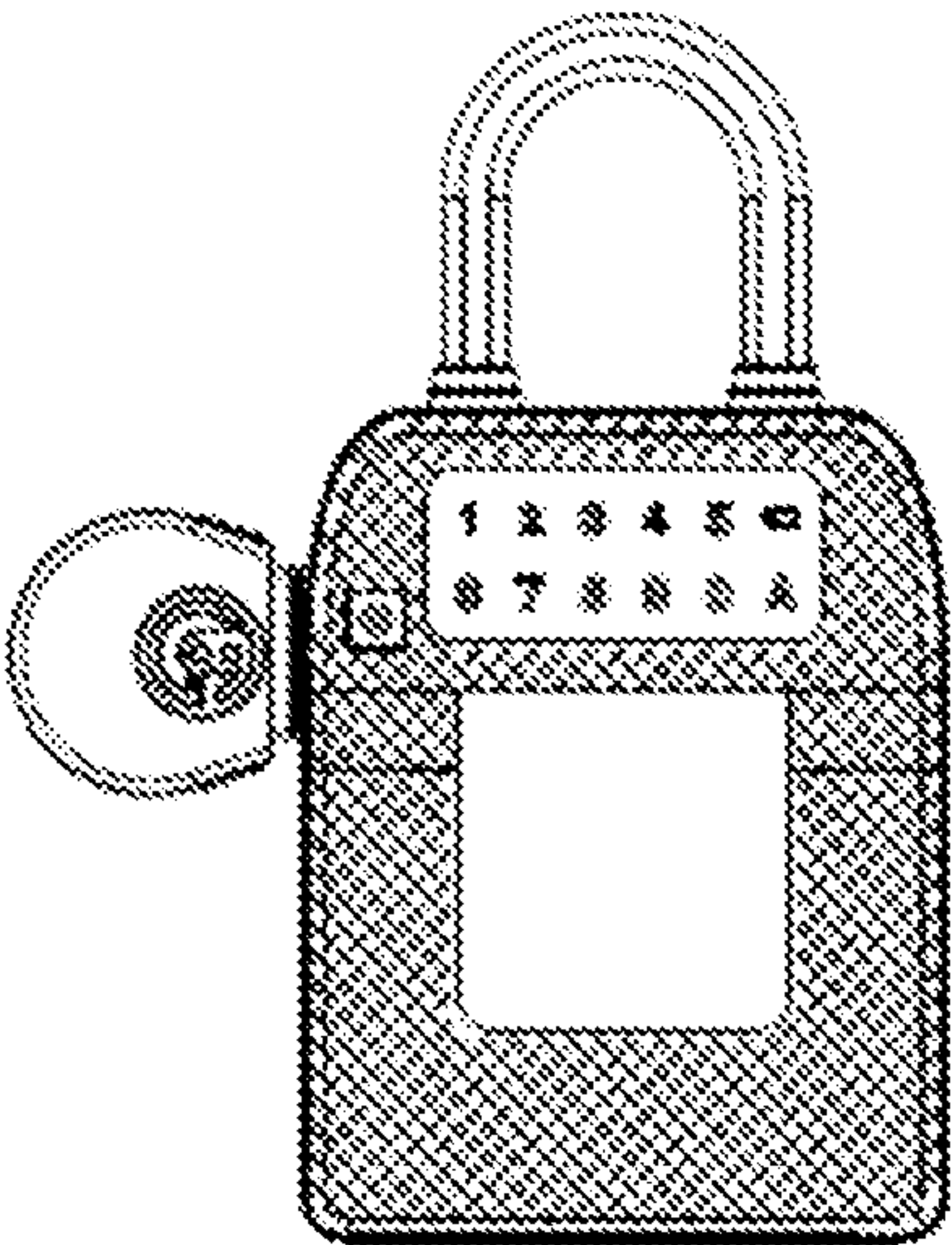


Fig. 13B

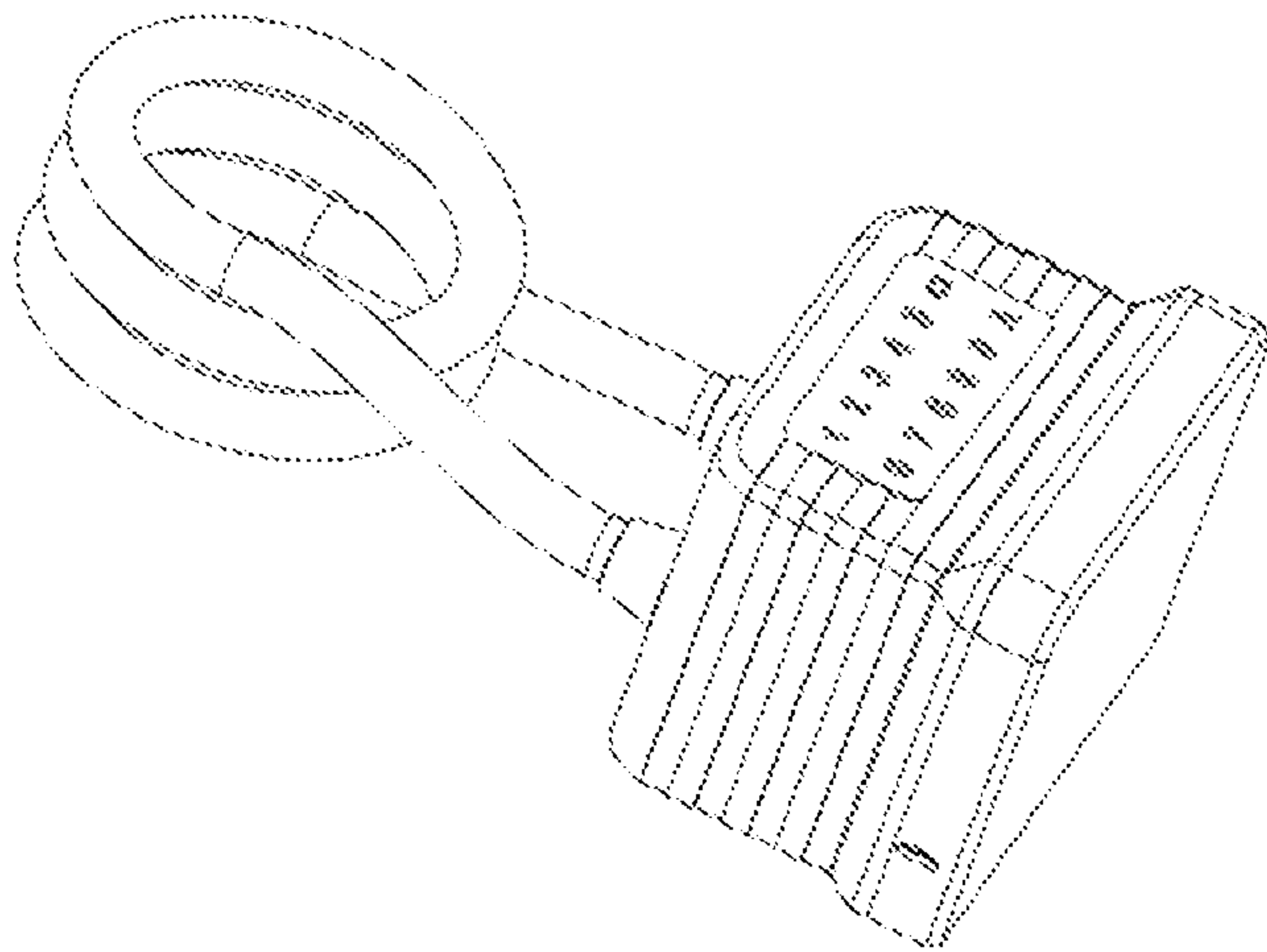


Fig. 14A

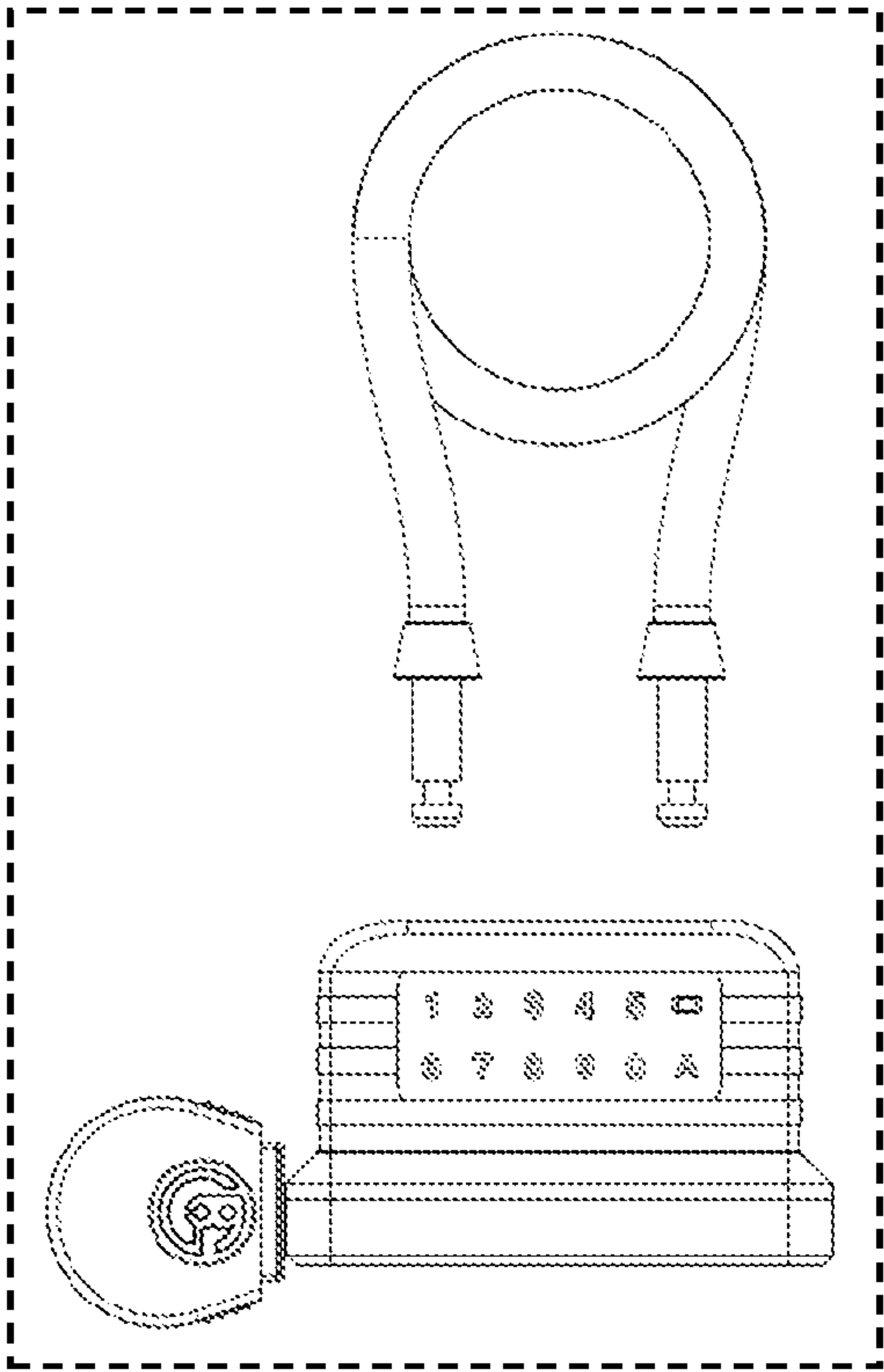


Fig. 14B

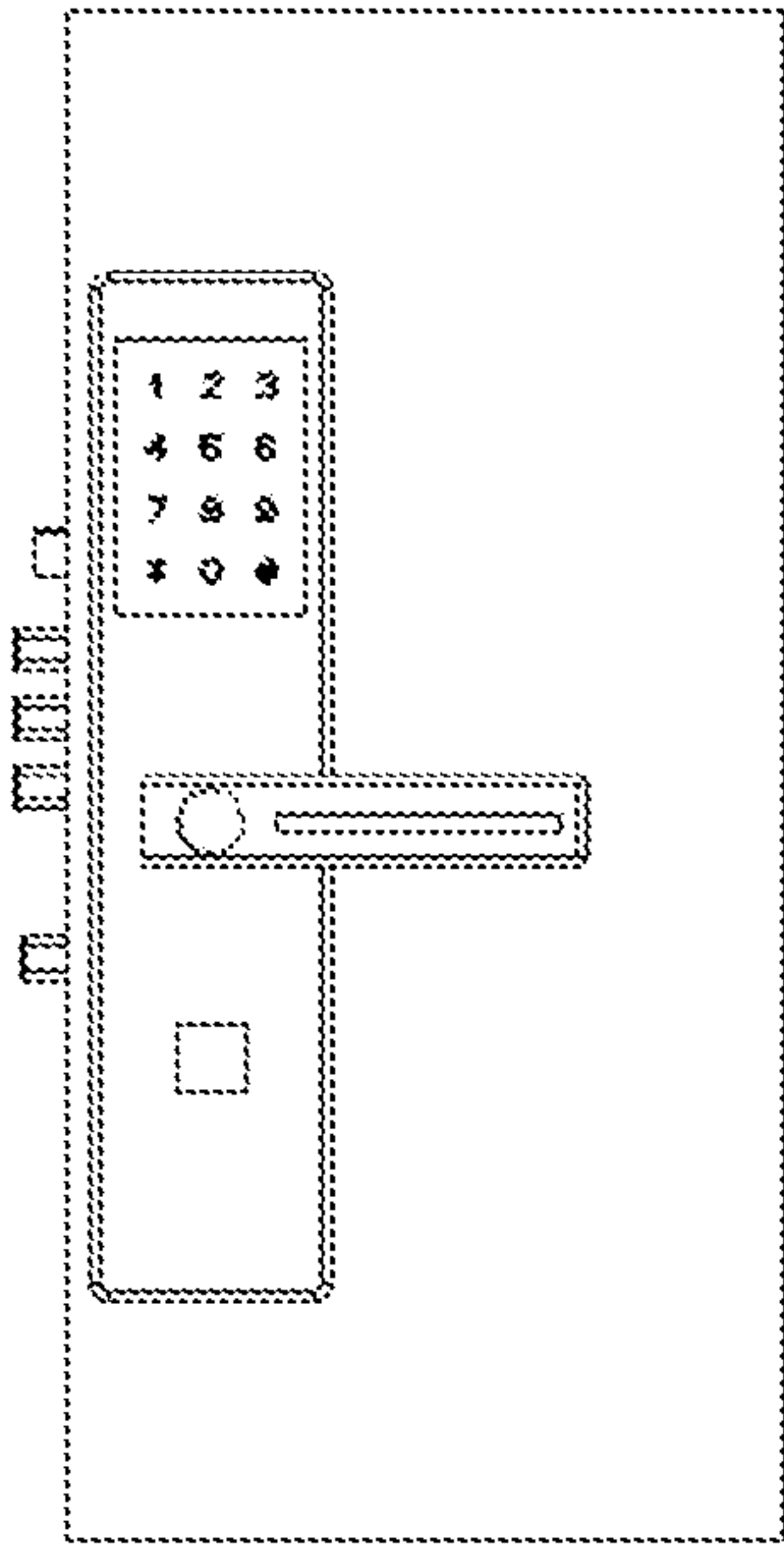


Fig. 15A

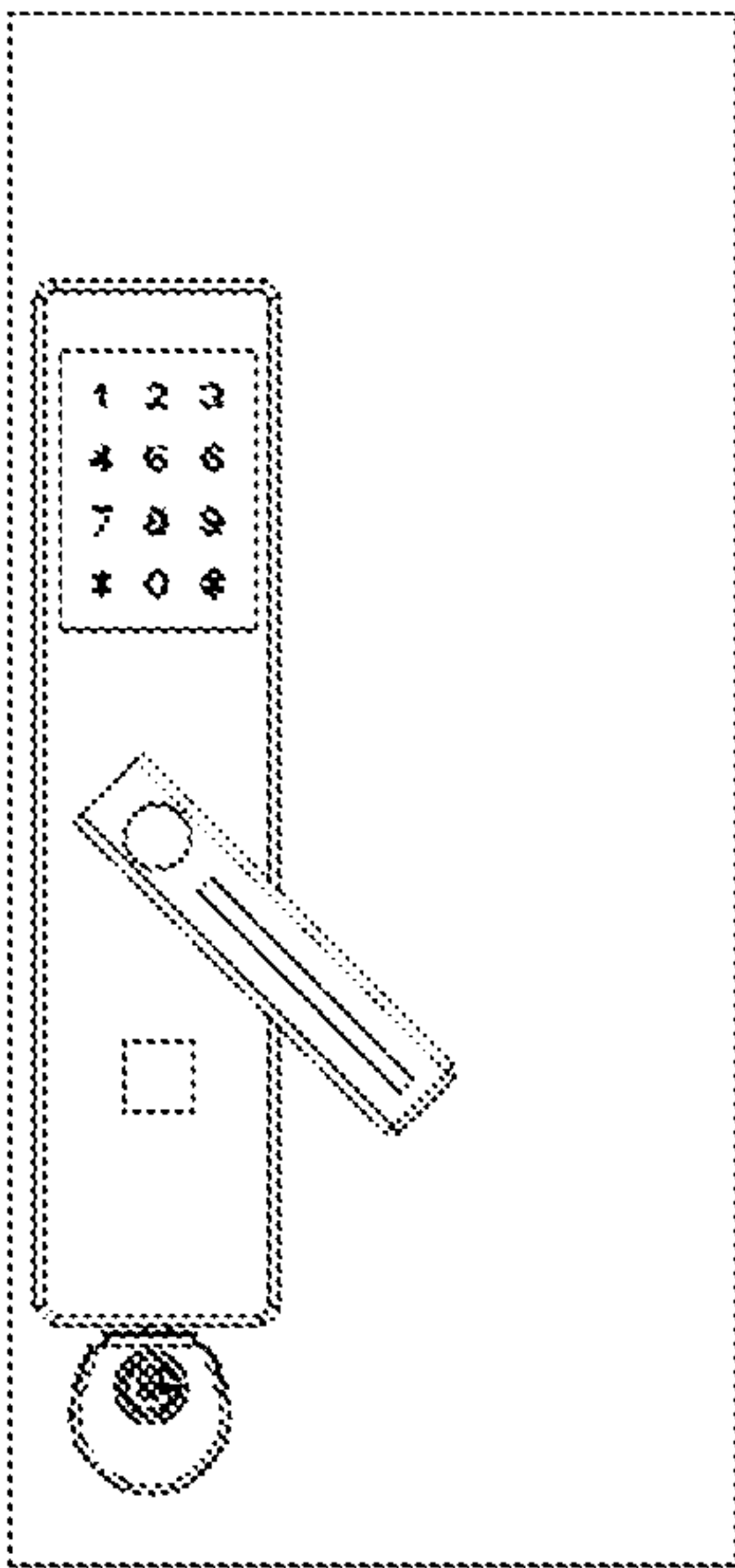


Fig. 15B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB2020/061882

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00(2020.01)i; E05B 47/00(2006.01)i; E05B 67/22(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)

G07C9/-;E05B47/-;E05B67/-;E05B19/-;E05B15/-

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)

CNABS,DWPL,SIPOABS,CNXTX,CNKI; KO, Ping Hon, lock+, unlock+, key?, control+, data, communication, port?, padlock?, bluetooth, power, wireless, wired

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 207761449 U (NANJING EASTHOUSE ELECTRICAL CO., LTD.) 24 August 2018 (2018-08-24) see description, paragraph 0027 to paragraph 0048, figures 1-7	1-22
X	CN 209585872 U (SHANGHAI SMURFS TECH. CO., LTD.) 05 November 2019 (2019-11-05) see description, paragraph 0022 to paragraph 0030, figures 1-3	1-22
A	CN 107404484 A (SHANGHAI AIYOUWEI SOFTWARE DEV. CO., LTD.) 28 November 2017 (2017-11-28) the whole document	1-22
A	CN 107313660 A (ANHUI DENUO TECH. CO., LTD.) 03 November 2017 (2017-11-03) the whole document	1-22
A	US 2018081335 A1 (VIDEX INC.) 22 March 2018 (2018-03-22) the whole document	1-22
A	WO 2018184070 A1 (ASSA ABLOY AUSTRALIA PTY. LTD.) 11 October 2018 (2018-10-11) the whole document	1-22

☐ 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

26 March 2021

Date of mailing of the international search report

15 April 2021

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC
6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

FANG,Jia

Telephone No. 86-(10)-53962836

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2020/061882

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	207761449	U	24 August 2018	CN	107939172	A	20 April 2018
CN	209585872	U	05 November 2019	None			
CN	107404484	A	28 November 2017	None			
CN	107313660	A	03 November 2017	None			
US	2018081335	A1	22 March 2018	US	9841743	B2	12 December 2017
				US	10423136	B2	24 September 2019
				US	2015287256	A1	08 October 2015
				US	2019361414	A1	28 November 2019
WO	2018184070	A1	11 October 2018	EP	3607160	A1	12 February 2020
				EP	3607160	A4	20 January 2021
				AU	2018247572	A1	10 October 2019
				US	2020165841	A1	28 May 2020