



(51) International Patent Classification:
H04L 9/08 (2006.01)

(21) International Application Number:
PCT/EP2021/082660

(22) International Filing Date:
23 November 2021 (23.11.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
20209445.4 24 November 2020 (24.11.2020) EP

(71) Applicant: JT INTERNATIONAL S.A. [CH/CH]; 8, rue
Kazem Radjavi, 1202 GENEVE (CH).

(72) Inventor: VERLAAN, Theodorus; Route de Florissant
16, 1206 GENEVE (CH).

(74) Agent: DOMENEGO, Bertrand et al.; LAVOIX, 2, place
d'Estienne d'Orves, 75441 Paris Cedex 09 (FR).

(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,

(54) Title: AEROSOL GENERATION DEVICE COMPRISING AN ELECTRONIC SYSTEM FOR GENERATING A RANDOM
ENCRYPTION KEY

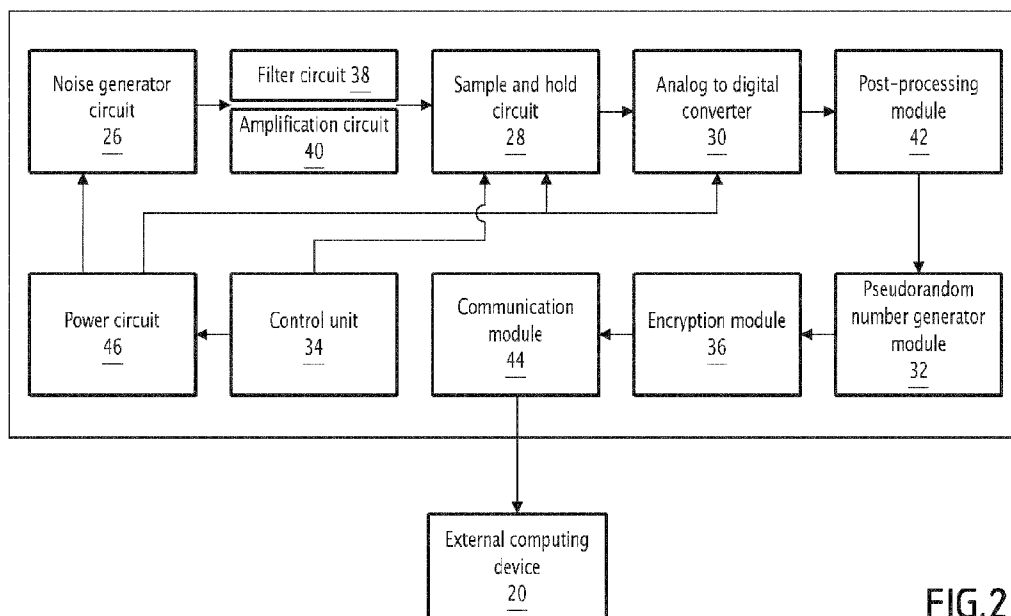


FIG.2

(57) Abstract: The invention concerns an aerosol generation device comprising an electronic system (16) for generating a random encryption key at a given instant. The system (16) comprises - a noise generator circuit (26) configured to generate an electrical noise; - a sample and hold circuit (28) configured to generate a sampled signal presenting a constant voltage equal to the voltage of the electrical noise at the given instant; - an analog to digital converter (30) configured to convert the sampled signal in a digital signal corresponding to the voltage of the sampled signal forming the value of a seed number; and - a pseudorandom number generator module (32) configured to generate a sequence of random numbers forming the encryption key based on the seed number.

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

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

**Aerosol generation device comprising an electronic system for generating a
random encryption key**

5

FIELD OF THE INVENTION

The present invention concerns an aerosol generation device comprising an electronic system for generating a random encryption key.

10

BACKGROUND OF THE INVENTION

15

Different types of aerosol generation assemblies are already known in the art. Generally, such assemblies comprise a storage portion for storing an aerosol forming precursor, which can comprise for example a liquid or a solid. A heating system is formed of one or more electrically activated resistive heating elements arranged to heat said precursor to generate the aerosol. The aerosol is released into a flow path extending between an inlet and outlet of the device. The outlet may be arranged as a mouthpiece, through which a user inhales for delivery of the aerosol.

20

25

In some aerosol generation assemblies, the precursor is stored in a removable cartridge. The aerosol generation assembly comprises then an aerosol generation device which defines a cavity in which the cartridge may be inserted. In order to attach the removable cartridge to the device body, a screw-threaded connection can for example be used. When the cartridge is assembled to the aerosol generation device, the device is able to generate the aerosol. When the precursor is consumed, the cartridge can be easily removed and replaced.

30

35

Some known aerosol generation devices comprise communication means with an external device such as a user's smartphone to communicate user data to the external device or operational settings to the aerosol generation device. The importance of secure data transmission from and to the aerosol generation device becomes therefore crucial. The information exchanged between the aerosol generation device and the external device is considered to be sensitive by users. For example, usage data such as duration, timings, locations, etc., is considered personal data and users are not accepting data transfer modes that are susceptible to attacks, like eavesdropping.

As aerosol generation devices are typically low cost and have real limitations with respect to power usage, any data encryption needs to be implemented with low hardware costs and have low energy requirements. In particular, power is limited in the aerosol generation device due to battery size, and most energy will be allocated to the core function of the aerosol generation device, namely powering the heating structure.

Communication standards do often include encryption, but as these are per definition standard, they are also big targets for being compromised. Therefore, there is an inherent risk associated to the standard encryption.

The data itself can also be encrypted to ensure that even if the data transmission protocol is compromised, the data retrieved in an attack is still encrypted and therefore safe. The simple way to protect data is to use a fixed encryption that is the same for each transmission. Implementation is easy and straightforward, with minimal hardware and processing costs. There is however a risk that once a single transmission is intercepted and decrypted, all subsequent transmissions are also compromised.

To that end, most of encryption methods use a changing encryption key. In cryptography, a key is a parameter that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms.

Known methods used for generating a key are based on algorithms that can generate an encryption key based on a seed. These algorithms are known in the art. By using random seeds, a random encryption key can be obtained.

There is therefore a need for an aerosol generation device able to generate an encryption key, in a random way and with low hardware costs and low energy requirements.

SUMMARY OF THE INVENTION

One of the aims of the present invention is therefore to provide an aerosol generation device able to generate a random encryption key with a low power

consumption and low hardware costs, in order to enable a safe communication between the aerosol generation device and an external computing device.

For this purpose, the invention relates to an aerosol generation device comprising an electronic system for generating a random encryption key at a given instant, the system comprising: a noise generator circuit configured to generate an electrical noise; a sample and hold circuit configured to generate a sampled signal presenting a constant voltage equal to the voltage of the electrical noise at the given instant; an analog to digital converter configured to convert the sampled signal in a digital signal corresponding to the voltage of the sampled signal forming the value of a seed number; and a pseudorandom number generator module configured to generate a sequence of random numbers forming the encryption key based on the seed number.

Indeed, using these features, the aerosol generation device is able to generate a random encryption key with very low power consumption and hardware expense thanks to the different components that are low cost and low power consumer. In particular, the noise generator circuit enables to provide some randomness in an easy and low power way.

According to some embodiments, the system further comprises a control unit configured to command the sample and hold circuit to generate the sampled signal at the given instant.

By implementing this feature, the aerosol generation device makes it possible to control when the encrypted key is generated.

According to some embodiments, the system further comprises further an encryption module able to encrypt data, notably the aerosol generation device user's data, based on the encryption key.

By implementing this feature, the aerosol generation device makes it possible to encrypt data which may be sensitive to protect them from possible external attacks.

According to some embodiments, the aerosol generation device comprises a communication module configured to send the encrypted data to an external computing

device via an encrypted transfer protocol, notably a short-range encrypted transfer protocol.

By implementing this feature, the aerosol generation device makes it possible to send the encrypted data to the external computing device in a safe and secured manner to guarantee the confidentiality of user data.

According to some embodiments, the communication module is configured to send the encryption key to the external computing device, notably via a Diffie-Hellman key-exchange protocol.

By implementing this feature, the aerosol generation device makes it possible to send the encryption key to the external computing device so the encrypted data may be decrypted and read by the external computing device.

According to some embodiments, the noise generator circuit is configured to generate a white electronic noise presenting a substantially flat frequency spectrum.

By implementing this feature, a better randomness of the number obtained. White noise circuits are also easy to implement.

According to some embodiments, the pseudorandom number generator is based on a linear-feedback shift register.

By implementing this feature, the pseudorandom number generator is able to generate random numbers in an easy and efficient manner.

According to some embodiments, the system further comprises a filter circuit configured to limit the bandwidth of the electrical noise.

According to some embodiments, the system further comprises an amplification circuit configured to amplify the electrical noise.

By implementing these features, the electrical noise may be filtered and/or amplified so that the sample and hold circuit may process correctly said electrical noise.

According to some embodiments, the system further comprises a post-processing module configured to verify if the seed number is within a predetermined range associated to the pseudorandom number generator module.

5 By implementing this feature, the seed number is controlled so that the pseudorandom number generator module may correctly generate the sequence of random numbers based on said seed number.

10 According to some embodiments, the aerosol generation device comprises further a power circuit configured to power the noise generator circuit, the sample and hold circuit and the analog to digital converter.

15 By implementing this feature, the aerosol generation device makes it possible to control the powering of the system in order to switch off the system when it is not needed for example.

The invention also relates to a method for generating a random encryption key for an aerosol generation device at a given instant, the method comprising at least the following steps:

- 20 - generating an electrical noise;
- sampling the electrical noise to generate a sampled signal presenting a constant voltage equal to the voltage of the electrical noise at the given instant;
- converting the sampled signal in a digital signal forming the value of a seed number; and
25 - generating the encryption key based on the seed number.

According to some embodiments, the method further comprises a step of encryption data, notably the aerosol generation device user's data, based on the encryption key.

30 According to some embodiments, the method further comprises a step of sending the encrypted data to an external computing device via an encrypted transfer protocol, notably a short-range encrypted transfer protocol.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention and its advantages will be better understood upon reading the following description, which is given solely by way of non-limiting example and which is made with reference to the appended drawings, in which:

- Figure 1 is a schematic diagram of an aerosol generation device according to the invention comprising an electronic system for generating a random encryption key and communicating with an external computing device,

- Figure 2 shows a schematic diagram of the electronic system of Figure 1, and

- Figure 3 shows a flowchart of a method, according to the invention, for generating a random encryption key carried out by the electronic system of Figure 2.

DETAILED DESCRIPTION OF THE INVENTION

Before describing the invention, it is to be understood that it is not limited to the details of construction set forth in the following description. It will be apparent to those skilled in the art having the benefit of the present disclosure that the invention is capable of other embodiments and of being practiced or being carried out in various ways.

As used herein, the term **“aerosol generation device”** or **“device”** may include a vaping device to deliver an aerosol to a user, including an aerosol for vaping, by means of aerosol generating unit (e.g. an aerosol generating element which generates vapor which condenses into an aerosol before delivery to an outlet of the device at, for example, a mouthpiece, for inhalation by a user). The device may be portable. “Portable” may refer to the device being for use when held by a user. The device may be adapted to generate a variable amount of aerosol, e.g. by activating a heater system for a variable amount of time (as opposed to a metered dose of aerosol), which can be controlled by a trigger. The trigger may be user activated, such as a vaping button and/or inhalation sensor. The inhalation sensor may be sensitive to the strength of inhalation as well as the duration of inhalation to enable a variable amount of vapor to be provided (so as to mimic the effect of smoking a conventional combustible smoking article such as a cigarette, cigar or pipe, etc.). The device may include a temperature regulation control to drive the temperature of the heater and/or the heated aerosol generating substance (aerosol pre-cursor) to a specified target temperature and thereafter to maintain the temperature at the target temperature that enables efficient generation of aerosol.

As used herein, the term “**aerosol**” may include a suspension of precursor as one or more of: solid particles; liquid droplets; gas. Said suspension may be in a gas including air. Aerosol herein may generally refer to/include a vapor. Aerosol may include one or more components of the precursor.

As used herein, the term “**aerosol-forming precursor**” or “**precursor**” or “**aerosol-forming substance**” or “**substance**” or “**vaporizable material**” is used to designate any material that is vaporizable in air to form aerosol. Vaporisation is generally obtained by a temperature increase up to the boiling point of the vaporization material, such as at a temperature up to 400°C, preferably up to 350°C. The vaporizable material may, for example, comprise or consist of an aerosol-generating liquid, gel, or wax or the like or an aerosol -generating solid that may be in the form of a rod, which contains processed tobacco material, a crimped sheet or oriented strips of reconstituted tobacco (RTB), or any combination of these. The vaporizable material may comprise one or more of: nicotine; caffeine or other active components. The active component may be carried with a carrier, which may be a liquid. The carrier may include propylene glycol or glycerin. A flavoring may also be present. The flavoring may include Ethylvanillin (vanilla), menthol, Isoamyl acetate (banana oil) or similar.

As used herein, the term “**external device**” may refer to a device, which is able to establish a wireless data connection with the aerosol generation device as it is explained in the specification. Such an external device may be a mobile device like a mobile phone for example. Additionally, such an external device may be a smart device able to process at least some data received from the aerosol generation device or intended to be transmitted to the aerosol generation device. Such a smart device can be a smartphone, a smartwatch, a tablet computer, a laptop, a desktop computer or any other smart object implemented for example according to the IoT (“Internet of things”) technology. Such a smart device can be also another aerosol generation device similar to said aerosol generation device.

DESCRIPTION OF AN EMBODIMENT OF THE INVENTION

The aerosol generation device 10 according to the invention is shown on Figure 1. In the example of this Figure 1, the aerosol generation device 10 is designed to operate with a removable cartridge (not showed) which is intended to be received in a payload

compartment 14. The cartridge comprises a precursor storage portion able to store a precursor and at least a heater able to heat the precursor to generate aerosol. The heater of the cartridge is connected electrically to a power source of the device 10 through a pair of contacts arranged in both cartridge and aerosol generation device 10. According to
5 another embodiment of the invention, the heater of the cartridge may be coupled with a heating element arranged in the device 10 and powered by the power source of this device 10. In this case, heat is transmitted directly from the heating element of the device to the heater of the cartridge. According to still another embodiment of the invention, the payload compartment 14 defines a fixed, in respect to the device 10, precursor storage
10 portion. In this case, the precursor storage portion can for example be refilled with a precursor.

As shown on Figure 1, the aerosol generation device 10 according to the invention comprises an electronic system 16 for generating a random encryption key. The aerosol
15 generation device 10 further comprises advantageously an antenna 22 for communication with an external computing device 20 and a battery cell 24, for example a rechargeable lithium-ion battery known in the art. The battery cell 24 is connected to a connector able to receive an external power supply signal adapted to charge the battery cell 24.

The random encryption key is for example designed to be used in a symmetric-key algorithm. Symmetric encryption is a type of encryption where only one key is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the encryption key so that it can be used in the decryption process by the receiver. This encryption method differs from asymmetric encryption where
25 a pair of keys, one public and one private, is used to encrypt and decrypt messages. By using symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret encryption key to decrypt it. Once the intended recipient who possesses the key has the message, the symmetric-key algorithm reverses its action so that the message is returned to its original and
30 understandable form.

According to another embodiment, the random encryption key is used in an asymmetric encryption process. In this case, the encryption key (also called the public key) and the corresponding decryption key (also called the private key) are different. A
35 message encrypted with the public key can be decrypted only with the corresponding private key. The public key and the private key are related mathematically, but it is

computationally infeasible to derive the private key from the public key. Therefore, a recipient could distribute the public key widely. Anyone can use the public key to encrypt messages for the recipient and only the recipient can decrypt them.

5 In reference to Figure 2, the electronic system 16 comprises a noise generator circuit 26, a sample and hold circuit 28, an analog to digital converter 30 and a pseudorandom number generator module 32. The electronic system 16 further comprises advantageously a control unit 34, an encryption module 36, a filter circuit 38, an amplification circuit 40, a post-processing module 42, a communication module 44 and a
10 power circuit 46.

The noise generator circuit 26 is configured to generate an electrical noise. Noise generator circuits are known by the skilled person. Several circuits may be used for noise generation. For example, the noise generator circuit 26 may comprise one of:
15 temperature-controlled resistors, temperature-limited vacuum diodes or zener diodes. Advantageously, the noise generator circuit 26 is configured to generate a white electronic noise. White noise presents a substantially flat frequency spectrum. In other words, white noise is a random signal having equal intensity at different frequencies, giving it a constant power spectral density.

20 The filter circuit 38 is configured to receive the electric noise from the noise generator circuit 26 and to limit the bandwidth of this electrical noise before transmitting the filtered signal to the sample and hold circuit 28. Any suitable filter can be used, high pass, low pass, band pass or combination thereof. The steepness of the filter may be
25 adjusted by the skilled person to obtain the desired random key generation.

The amplification circuit 40 is configured to amplify the electrical noise. The amplification circuit 40 may be arranged before or after the filter circuit 38. In particular, the amplification circuit 40 is configured to amplify the electrical noise if the amplitude of
30 the electrical noise is too low for the sample and hold circuit 28 to process correctly said electrical noise.

The sample and hold circuit 28 is configured to generate a sampled signal presenting a constant voltage equal to the voltage of the electrical noise at a given instant.
35 As it will be described below, the given instant is the instant when the encryption key generation is requested, notably by the control unit 34. The sample and hold circuit 28 is

configured to sample the voltage of the continuously varying analog signal generated by the noise generator circuit 26 and holds its value at a constant level for a specified minimum period of time. The sample and hold circuit 28 stores electric charge in a capacitor and contains at least one switching device such as a field effect transistor switch and optionally one operational amplifier. To sample the input signal the switch connects the capacitor to the output of a buffer amplifier. The buffer amplifier charges or discharges the capacitor so that the voltage across the capacitor is practically equal, or proportional to, input voltage.

The analog to digital converter 30 is configured to convert the sampled signal in a digital signal corresponding to the voltage of the sampled signal forming the value of a seed number. Several architectures for the analog-to-digital converter 30 are known by the skilled person. For example, the analog to digital converter 30 presents a flash architecture, a pipelined architecture, a successive approximations architecture or a sigma-delta architecture.

The post-processing module 42 is configured to receive the seed by the analog to digital converter 30 and verify if the seed number is within a predetermined range associated to the pseudorandom number generator module 32. If the seed number is within the predetermined range, the seed number is sent to the pseudorandom number generator module 32. If not, the post-processing module 42 blocks the transmission of the seed number.

The pseudorandom number generator module 32 is configured to generate a sequence of random numbers forming the encryption key based on the seed number. By "random numbers" it is understood numbers whose properties approximate the properties of sequences of random numbers. The skilled person will understand that the numbers generated by a pseudorandom number generator cannot be truly random, as the generated sequence is completely determined by an initial value. The skilled person will understand that a "sequence of random number" is therefore a sequence of numbers that is sufficiently close to random to suit the intended use of cryptography. A random number generator is an algorithm that, based on the initial seed number, produces a sequence of numbers or respectively bits, the sequence appearing random to any observer.

Advantageously, the pseudorandom number generator 32 is based on a linear-feedback shift register. A linear feedback shift register is composed of a shift register R

which contains a sequence of bits and a feedback function f which is the bit sum (xor) of a subset of the entries of the shift register. The shift register contains n memory cells, or stages, labelled $R_{n-1}, \dots, R_1, R_0$, each holding one bit. Each time a bit is needed the entry in stage R_0 is output while the entry in cell R_i is passed to cell R_{i-1} and the top stage R_{n-1} is updated with the value $f(R)$. Advantageously, the linear feedback shift register comprises 8, 16 or 32 bits.

The control unit 34 is configured to command the sample and hold circuit 28 to generate the sampled signal at the given instant. The control unit 34 is further configured to control the power circuit 46. The power circuit 46 is configured to power the noise generator circuit 26, the sample and hold circuit 28 and the analog to digital converter 30. In particular, the power circuit 46 is connected to the battery 24 in order to provide electricity to the noise generator circuit 26, the sample and hold circuit 28 and the analog to digital converter 30.

The control unit 34 is configured to control the activation of the power circuit 46 when the generation of an encryption key is needed. In particular, the control unit 34 is configured to command the generation of a new encryption key.

In a first embodiment, the control unit 34 is configured to command the generation of a new encryption key for each data transmission. This solution is the safest way to transmit the data, for example to transmit batches of data, like logs of device information.

In a variant or in complement, the control unit 34 is configured to command the generation of a new encryption key each time the device 10 gets powered on, or reactivation after entering a sleep/suspended mode. In this way, each time an event like a vaping session is started, the encryption key is updated. In another variant or in complement, the control unit 34 is configured to command the generation of a new encryption key at the start and/or at the end of each vaping session. For example, the command by the control unit 34 is triggered by the device 10 initiating a heating cycle. In another variant, the control unit 34 is configured to command the generation of a new encryption key at regular intervals of time. For example, the control unit 34 is configured to command the generation of a new encryption key every 10 seconds, 15 minutes, each hour or once a day, depending on the level of security desired by the user and the confidentiality of the exchanged data. This solution is particularly advantageous when the communication between the aerosol generation device 10 and the external computing

device 20 is almost constant, regardless of the aerosol generation device 10 being in use for vaping.

5 The encryption module 36 is able to encrypt data, notably the aerosol generation device user's data, based on the encryption key, using an encryption algorithm. Such an encryption algorithm is known by the skilled person and corresponds for example to Triple DES, RSA, Blowfish or AES algorithm.

10 The communication module 44 is configured to send the encrypted data to an external computing device 20 via an encrypted transfer protocol, notably a short-range encrypted transfer protocol. By "short-range transfer protocol", it is understood a protocol able to transfer data over a few meters. The communication module 44 is configured to communicate with the external computing device 20 via the antenna 22. In particular, the communication module 44 is configured to communicate with the external computing
15 device 20 via an NFC protocol (Near-Field Communication protocol), an RFID protocol (Radio-frequency identification protocol), a Bluetooth protocol, a Wi-Fi protocol, a Zigbee protocol or a LoRaWAN protocol. Thus, the antenna 22 is configured to carry out radio signal transmission according to the corresponding data transmission protocol.

20 The communication module 44 is further configured to send the encryption key to the external computing device 20 so that the external computing device 20 may decrypt the transmitted data. In particular, the communication module 44 is configured to send the encryption key via a Diffie-Hellman key-exchange protocol. The Diffie-Hellman key exchange protocol, also known as exponential key exchange, is a digital encryption
25 method that relies on high numbers at given powers to obtain decryption keys based on components never directly transmitted in order to make any attempt to decipher the code mathematically insurmountable. Diffie-Hellman Key Exchange defines a secret key shared between two parties that can be used to secretly communicate and exchange data over a public network. This method uses public key techniques to exchange a private encryption
30 key.

35 In a variant, the communication module 44 is configured to send the encryption key without applying an additional encryption to the encryption key, relying only on the safety of the used transmission protocol. In this case, the encryption key is more vulnerable during transmission, but the calculation efforts for the aerosol generation device 10 are significantly reduced. Also, the critical transmission is short in time, reducing the risk.

Advantageously, the encryption key is generated again regularly, reducing the risk of sustained attacks.

In the example of Figure 2, the electronic system 16 comprises an information processing unit for example formed by a memory and a processor associated with the memory. In this example, each of the pseudorandom number generator module 32, the control unit 34, the encryption module 36, the post-processing module 42, the communication module 44 and the power circuit 46 is made in the form of software stored in the memory, or a software component, executable by the processor.

In a variant, each of the pseudorandom number generator module 32, the control unit 34, the encryption module 36, the post-processing module 42, the communication module 44 and the power circuit 46 is made in the form of a programmable logic component, such as an FPGA (Field Programmable Gate Array), or in the form of a dedicated integrated circuit, such as an ASIC (Application Specific Integrated Circuit). When the electronic system 16 is made in the form of one or several software programs, i.e., in the form of a computer program, it is further able to be stored on a medium, not shown, readable by computer. The computer-readable medium is for example a medium suitable for storing electronic instructions and able to be coupled with a bus of a computer system. As an example, the readable medium is an optical disc, a magnetic-optical disc, a ROM memory, a RAM memory, any type of non-volatile memory (for example, EPROM, EEPROM, FLASH, NVRAM), a magnetic card or an optical card. A computer program including software instructions is then stored on the readable medium.

The operation of the electronic system 16 will now be explained in reference to Figure 3 showing a flowchart of the method according to the invention, for generating a random encryption key, the method being implemented by the electronic system 16.

Initially, it is considered that the aerosol generation device 10 and an external computing device 20, such a smartphone, are provided to a user. It is also considered that data need to be send from the aerosol generation device 10 to the external computing device 20. For example, data is user data and is considered confidential. Therefore, the data sending need to be encrypted.

To this end, during a first step 100, the control unit 34 commands the power circuit 46 which powers the noise generator circuit 26, the sample and hold circuit 28 and the analog to digital converter 30. In particular, the control unit 34 commands the generation

of a new encryption key for each data transmission; at each time the aerosol generation device 10 gets powered on, or reactivated after entering a sleep/suspended mode; at the start and/or at the end of each vaping session; or at regular intervals of time.

5 Then, during step 110, an electrical noise is generated by the noise generator circuit 26. Advantageously, a white electronic noise is generated, presenting a substantially flat frequency spectrum.

10 During optional step 120, the filter circuit 38 filters the electric noise to limit the bandwidth of this electrical noise before transmitting the filtered signal to the sample and hold circuit 28.

15 If the amplitude of the electrical noise is too low for the sample and hold circuit 28 to process correctly the said electrical noise, during another optional step 130, the electrical noise is amplified by the amplification circuit 40.

Steps 120 and 130 may be carried out in any order after step 110 and before step 140.

20 Then, during next step 140, the control unit 34 commands the sample and hold circuit 28 to generate the sampled signal at the given instant. In particular, the sample and hold circuit 28 generates a sampled signal presenting a constant voltage equal to the voltage of the electrical noise at the given instant.

25 During next step 150, the sampled signal is converted in a digital signal forming the value of a seed number by the analog to digital converter 30.

30 The seed is received by the post-processing module 42 which verifies if the seed number is within a predetermined range associated to the pseudorandom number generator module 32, during optional step 160. If the seed number is within the predetermined range the seed number is send to the pseudorandom number generator module 32.

35 The method comprises then a step 170 of generating the encryption key based on the seed number. Advantageously, the pseudorandom number generator module 32 generates the encryption key using a linear-feedback shift register.

During next step 180, data is encrypted by the encryption module 36 based on the encryption key. In particular, the encryption module 36 encrypts aerosol generation device user's data. Therefore, data is thus protected and may be sent to the outside of the device 10, notably to the external computing device 20.

To that end, during step 190 the communication module 44 sends the encrypted data to the external computing device 20 via an encrypted transfer protocol, notably a short-range encrypted transfer protocol.

The communication module 44 sends also the encryption key to the external computing device 20, during step 200. In particular, the communication module 44 sends the encryption key via a Diffie-Hellman key-exchange protocol. The external computing device 20 may then use the encryption key to decrypt the transmitted encrypted data. The external computing device 20 may use the data to control the good operation of the aerosol generation device 10, alert the user when the amount of precursor is low in the precursor storage portion, advice the user based on his habits, etc.

It appears clear that the invention has a number of advantages. In particular, the invention enables to generate a random encryption with low hardware costs and power consumption. Indeed, the different components of the electronic system 16 are each low cost and low power consumer. In particular, the noise generator circuit 26 enables to provide some randomness in an easy and low power way. Moreover, the invention may be easily implemented in existing aerosol generation devices.

While there have been shown and described and pointed out the fundamental novel features of the invention as applied to certain inventive embodiments, it will be understood that the foregoing is considered as illustrative only of the principles of the invention and not intended to be exhaustive or to limit the invention to the precise forms disclosed. Modifications or variations are possible in light of the above teachings.

CLAIMS

1. An aerosol generation device (10) comprising an electronic system (16) for
5 generating a random encryption key at a given instant, the system (16) comprising:

- a noise generator circuit (26) configured to generate an electrical noise;
- a sample and hold circuit (28) configured to generate a sampled signal
10 presenting a constant voltage equal to the voltage of the electrical noise at the
given instant;
- an analog to digital converter (30) configured to convert the sampled signal in a
digital signal corresponding to the voltage of the sampled signal forming the value
of a seed number; and
- a pseudorandom number generator module (32) configured to generate a
15 sequence of random numbers forming the encryption key based on the seed
number.

2. The aerosol generation device (10) according to claim 1, wherein the system
(16) further comprises a control unit (34) configured to command the sample and hold
20 circuit (28) to generate the sampled signal at the given instant.

3. The aerosol generation device (10) according to claim 1 or 2, wherein the
system (16) further comprises further an encryption module (36) able to encrypt data,
notably the aerosol generation device (10) user's data, based on the encryption key.

4. The aerosol generation device (10) according to claim 3, further comprising a
25 communication module (44) configured to send the encrypted data to an external
computing device (20) via an encrypted transfer protocol, notably a short-range encrypted
transfer protocol.

5. The aerosol generation device (10) according to claim 4, wherein the
30 communication module (44) is configured to send the encryption key to the external
computing device (20), notably via a Diffie-Hellman key-exchange protocol.

6. The aerosol generation device (10) according to any one of the preceding
35 claims, wherein the noise generator circuit (26) is configured to generate a white
electronic noise presenting a substantially flat frequency spectrum.

7. The aerosol generation device (10) according to any one of the preceding claims, wherein the pseudorandom number generator (32) is based on a linear-feedback shift register.

5

8. The aerosol generation device (10) according to any one of the preceding claims, wherein the system (16) further comprises a filter circuit (38) configured to limit the bandwidth of the electrical noise.

10

9. The aerosol generation device (10) according to any one of the preceding claims, wherein the system (16) further comprises an amplification circuit (40) configured to amplify the electrical noise.

15

10. The aerosol generation device (10) according to any one of the preceding claims, wherein the system (16) further comprises a post-processing module (42) configured to verify if the seed number is within a predetermined range associated to the pseudorandom number generator module (32).

20

11. The aerosol generation device (10) according to any one of the preceding claims, comprising further a power circuit (46) configured to power the noise generator circuit (26), the sample and hold circuit (28) and the analog to digital converter (30).

25

12. A method for generating a random encryption key for an aerosol generation device (10) at a given instant, the method comprising at least the following steps:

- generating (110) an electrical noise;
- sampling (120) the electrical noise to generate a sampled signal presenting a constant voltage equal to the voltage of the electrical noise at the given instant;
- converting (150) the sampled signal in a digital signal forming the value of a seed number; and
- generating (170) the encryption key based on the seed number.

30

13. The method of generating according to claim 12 further comprising a step (180) of encryption data, notably the aerosol generation device (10) user's data, based on the encryption key.

35

14. The method of generating according to claim 13 further comprising a step (190) of sending the encrypted data to an external computing device (20) via an encrypted transfer protocol, notably a short-range encrypted transfer protocol.

1/3

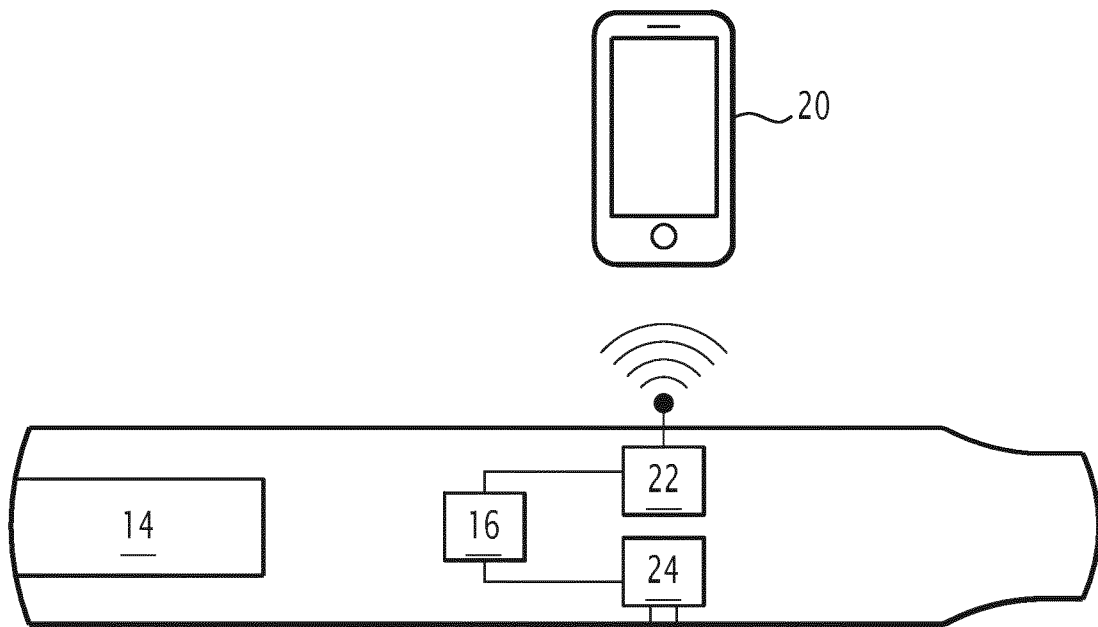


FIG.1

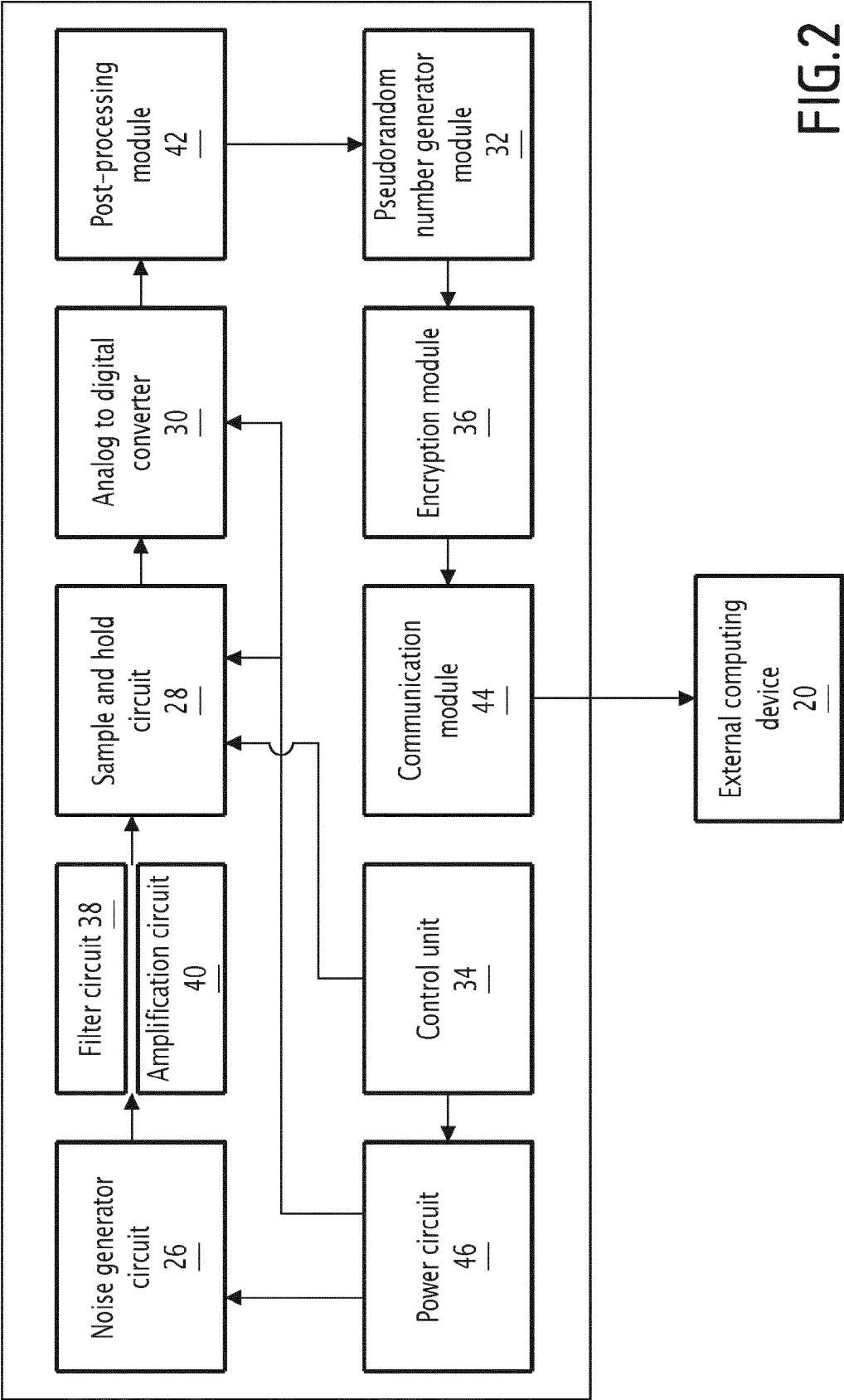
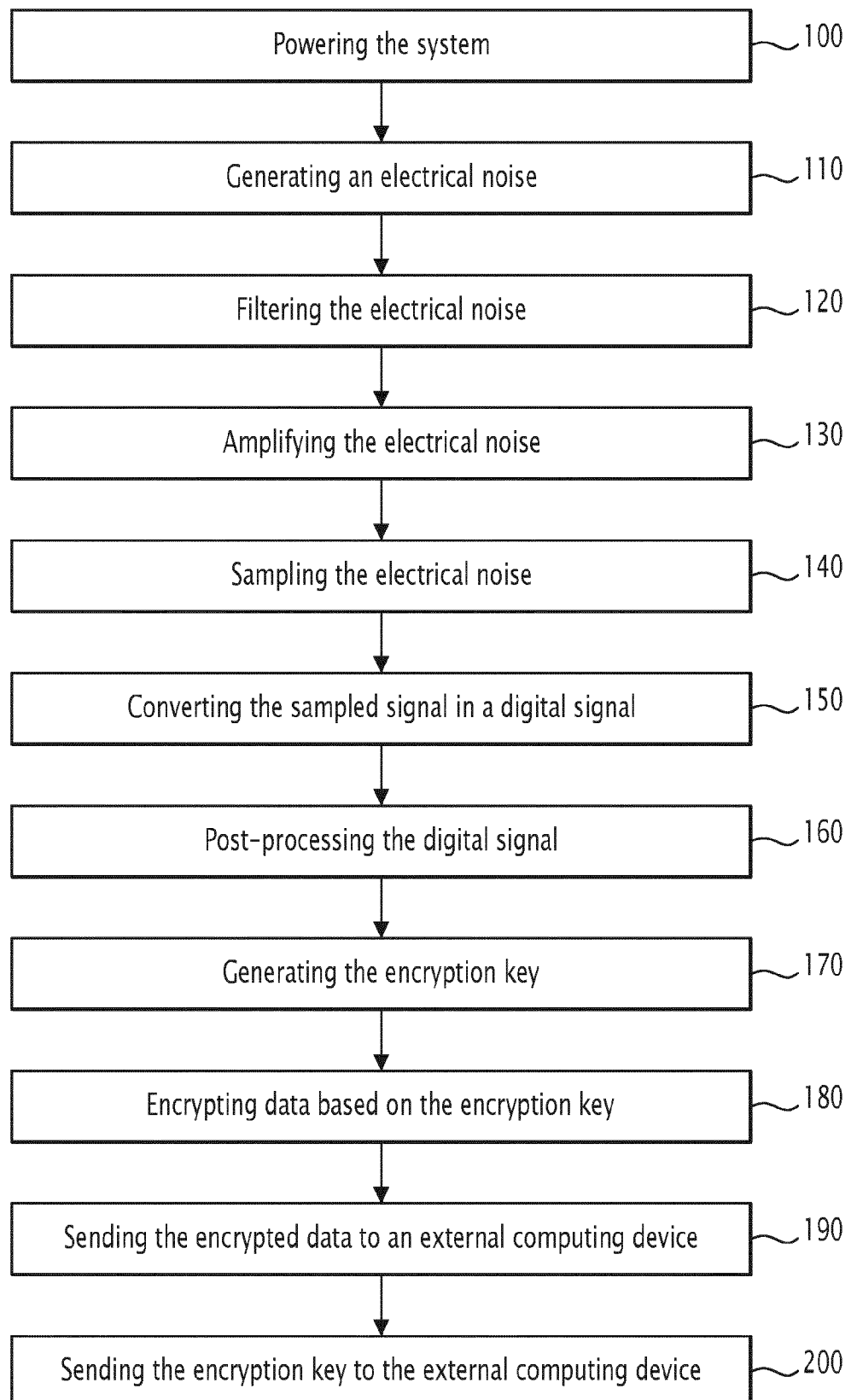


FIG. 2

FIG.3

3/3



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2021/082660

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/08 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) H04L		
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) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2020/176898 A1 (JUUL LABS INC [US]) 3 September 2020 (2020-09-03) paragraphs [0011], [0078]; figure 1a -----	1-14
Y	US 8 223 049 B2 (LARSEN FREDRIK [NO]; PEDERSEN FRODE MILCH [NO] ET AL.) 17 July 2012 (2012-07-17) column 6; figure 1 -----	1-14
Y	EP 2 654 208 A2 (LINEAR TECHNOLOGY CORP) 23 October 2013 (2013-10-23) paragraphs [0105] - [0106] ----- -/--	1-14
☒ 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 18 February 2022		Date of mailing of the international search report 01/03/2022
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Billet, Olivier

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2021/082660

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CALLEGARI S ET AL: "Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos", IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE SERVICE CENTER, NEW YORK, NY, US, vol. 53, no. 2, 1 February 2005 (2005-02-01), pages 793-805, XP011125218, ISSN: 1053-587X, DOI: 10.1109/TSP.2004.839924 section 1 -----	1-14

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2021/082660

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2020176898	A1	03-09-2020	NONE
US 8223049	B2	17-07-2012	NONE
EP 2654208	A2	23-10-2013	CN 103378861 A 30-10-2013
			CN 107809244 A 16-03-2018
			CN 107846223 A 27-03-2018
			EP 2654208 A2 23-10-2013
			TW 201345164 A 01-11-2013
			US 2013278453 A1 24-10-2013
			US 2014132430 A1 15-05-2014
			US 2014132431 A1 15-05-2014
			US 2014132432 A1 15-05-2014