(12) UK Patent (19) GB (11) 2538052 (13) B

(45) Date of B Publication 03.07.2019

(54) Title of the Invention: Encoder, decoder, encryption system, encryption key wallet and method

(51) INT CL: ***H04L 9/08*** (2006.01) ***G06F 21/62*** (2013.01) ***G06Q 20/36*** (2012.01)

(21) Application No: **1507154.1**

(22) Date of Filing: **27.04.2015**

(43) Date of A Publication **09.11.2016**

(56) Documents Cited:

WO 2014/108182 A
JP 2009032003 A
US 20140040147 A
US 20110271279 A
US 20020141575 A
WO 2002/029557 A
US 20140380047 A
US 20130326233 A
US 20090034733 A

(58) Field of Search:

As for published application 2538052 A viz:
INT CL **G06F, H04L, H04W**
Other: **ONLINE: WPI, EPODOC**
updated as appropriate

Additional Fields
INT CL **G06Q**

(72) Inventor(s):

Tuomas Kärkkäinen
Ossi Kalevo

(73) Proprietor(s):

Gurulogic Microsystems Oy
Linnankatu 34, Turku FI-20100, Finland

(74) Agent and/or Address for Service:

Basck Ltd
16 Saxon Road, CAMBRIDGE, Cambridgeshire, CB5 8HS, United Kingdom

GB 2538052 B

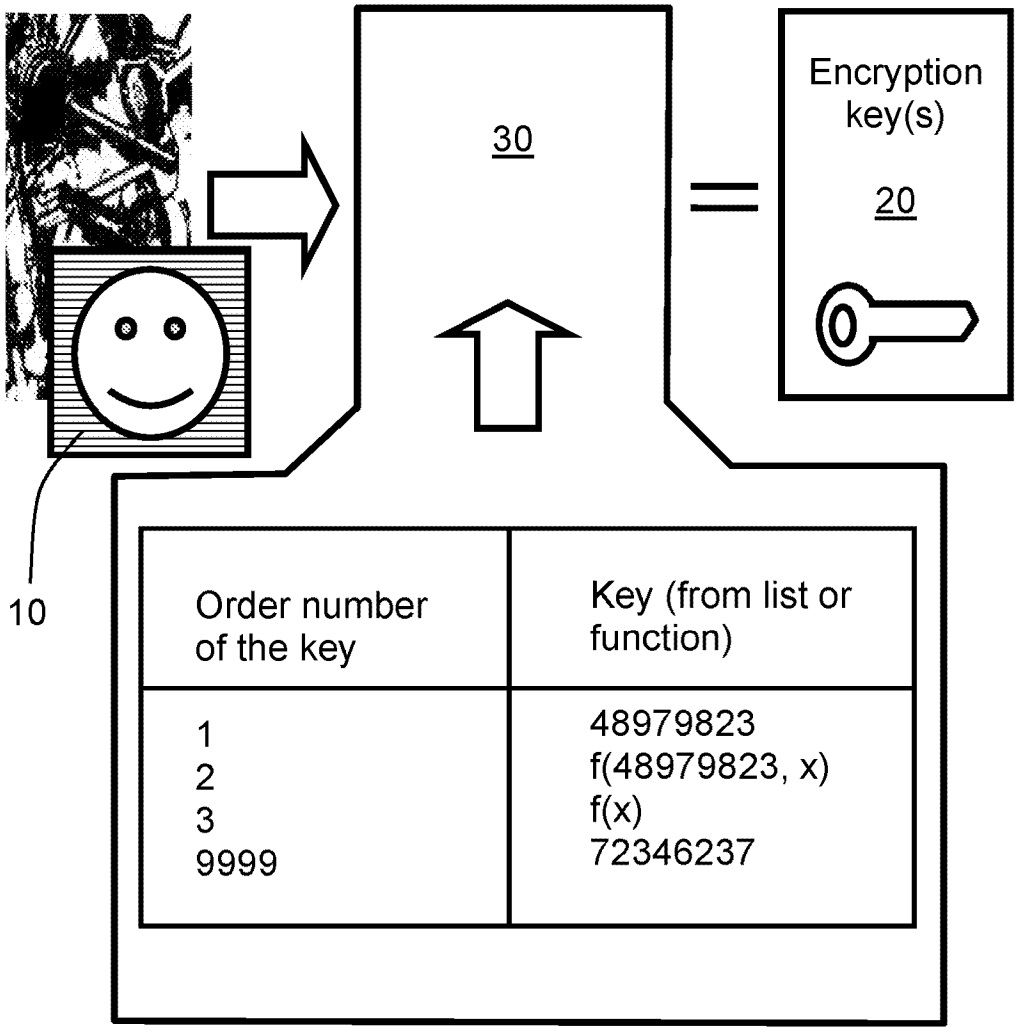
30
Encryption key(s)
20
10
Order number of the key
Key (from list or function)
1
2
3
9999
48979823
f(48979823, x)
f(x)
72346237

FIG. 1a

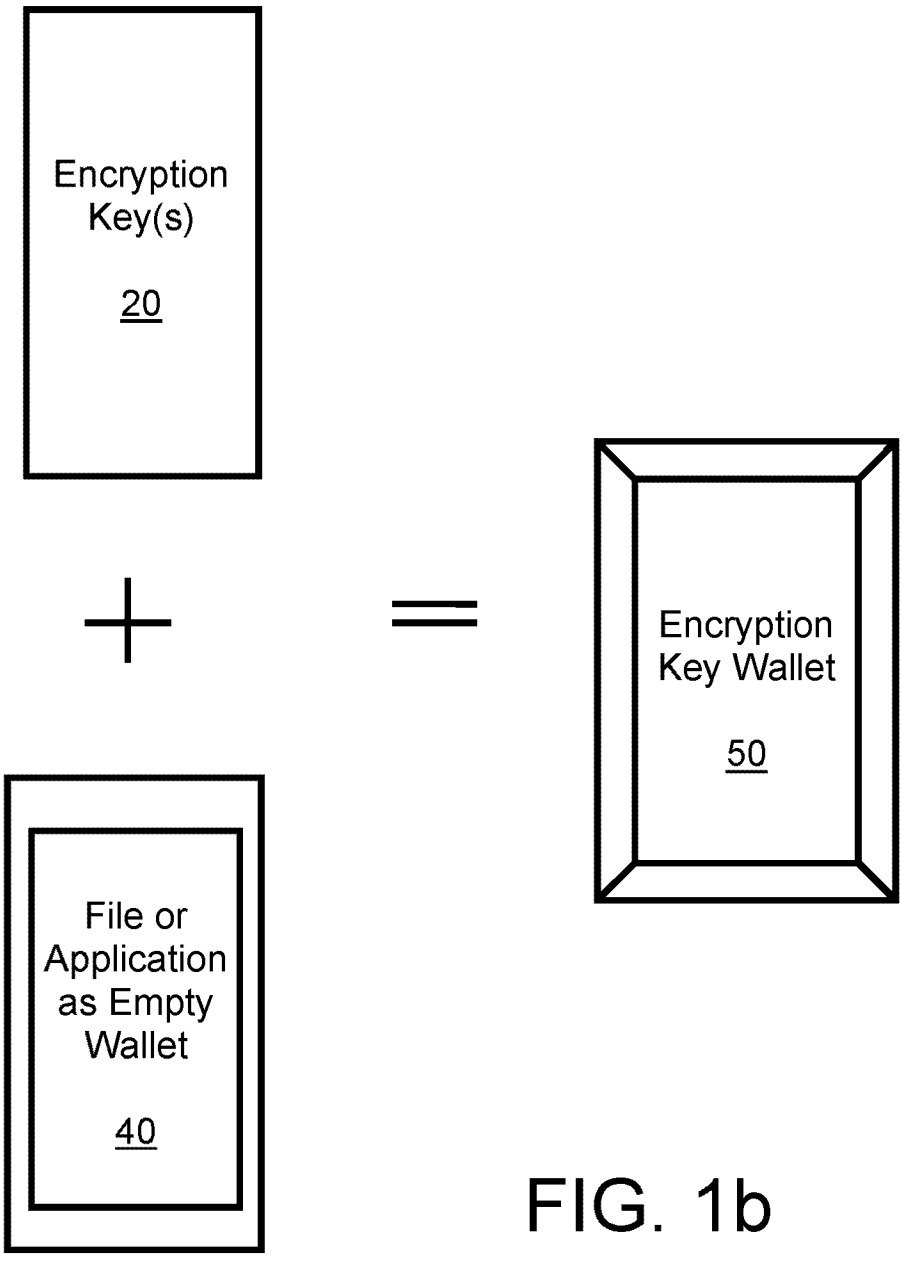
Encryption Key(s)
20
+
File or Application as Empty Wallet
40
=
Encryption Key Wallet
50

FIG. 1b

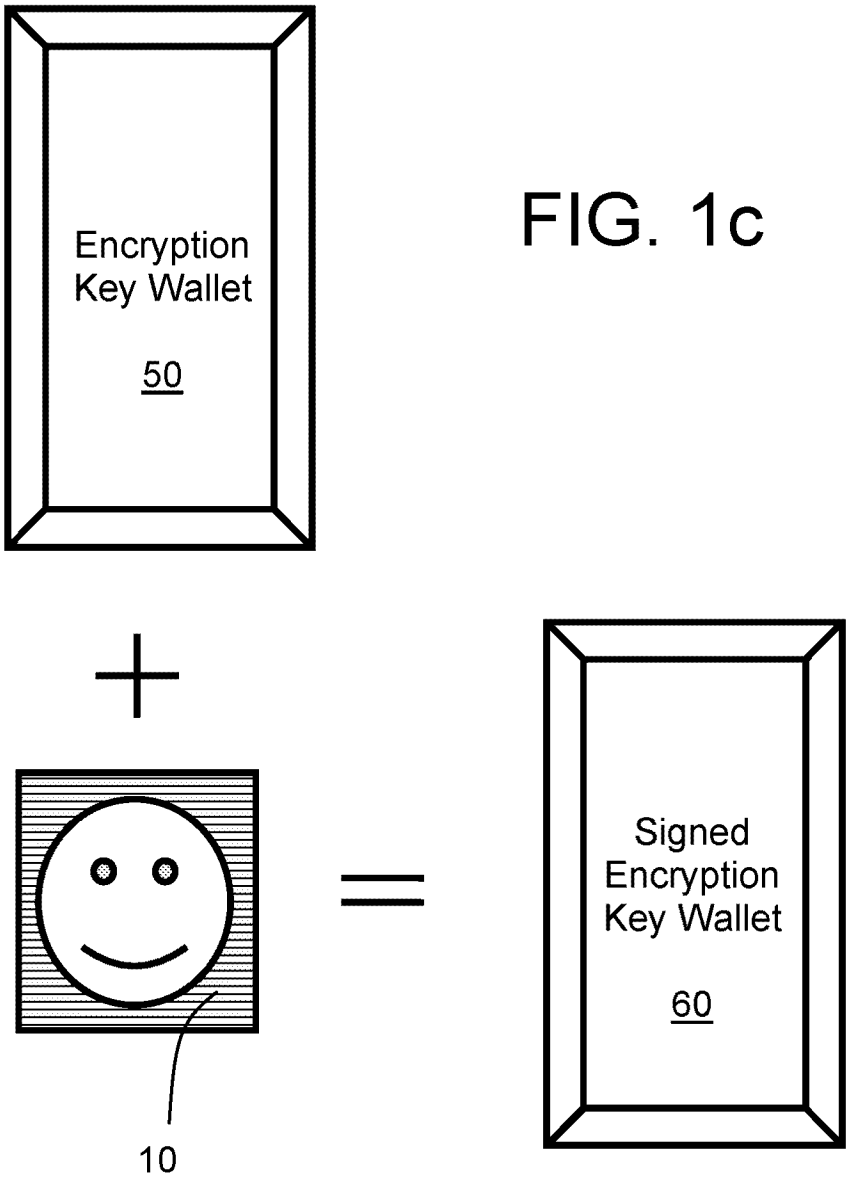
Encryption
Key Wallet
50
10
Signed
Encryption
Key Wallet
60

FIG. 1c

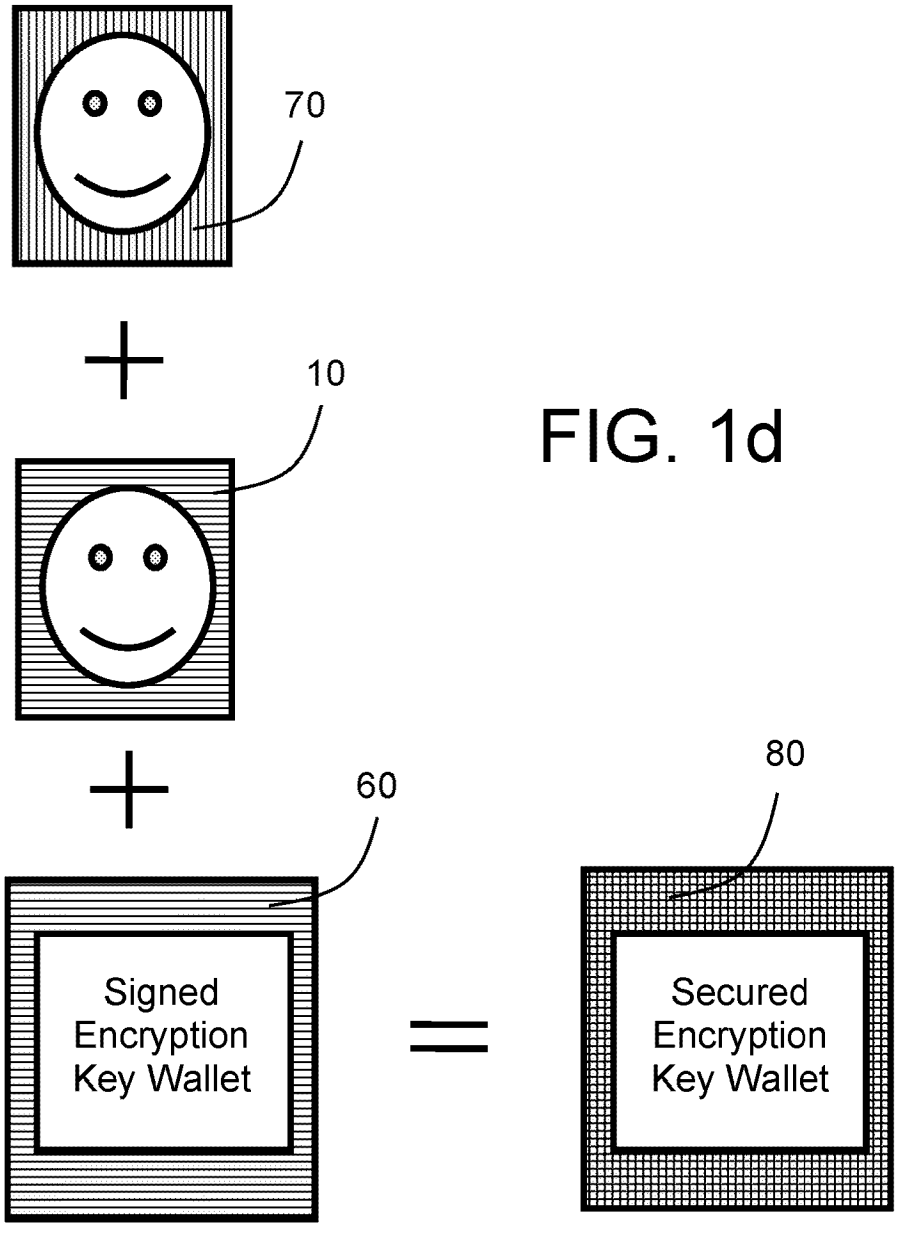
70
10
60
Signed
Encryption
Key Wallet
80
Secured
Encryption
Key Wallet

FIG. 1d

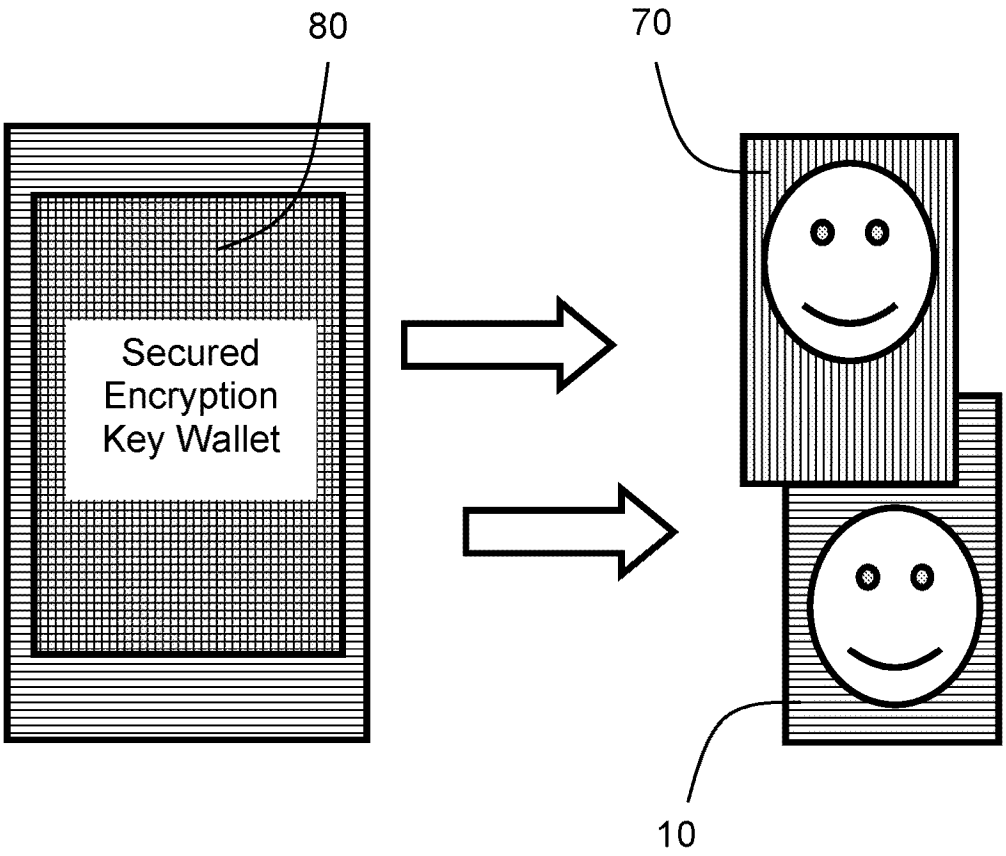

FIG. 1e

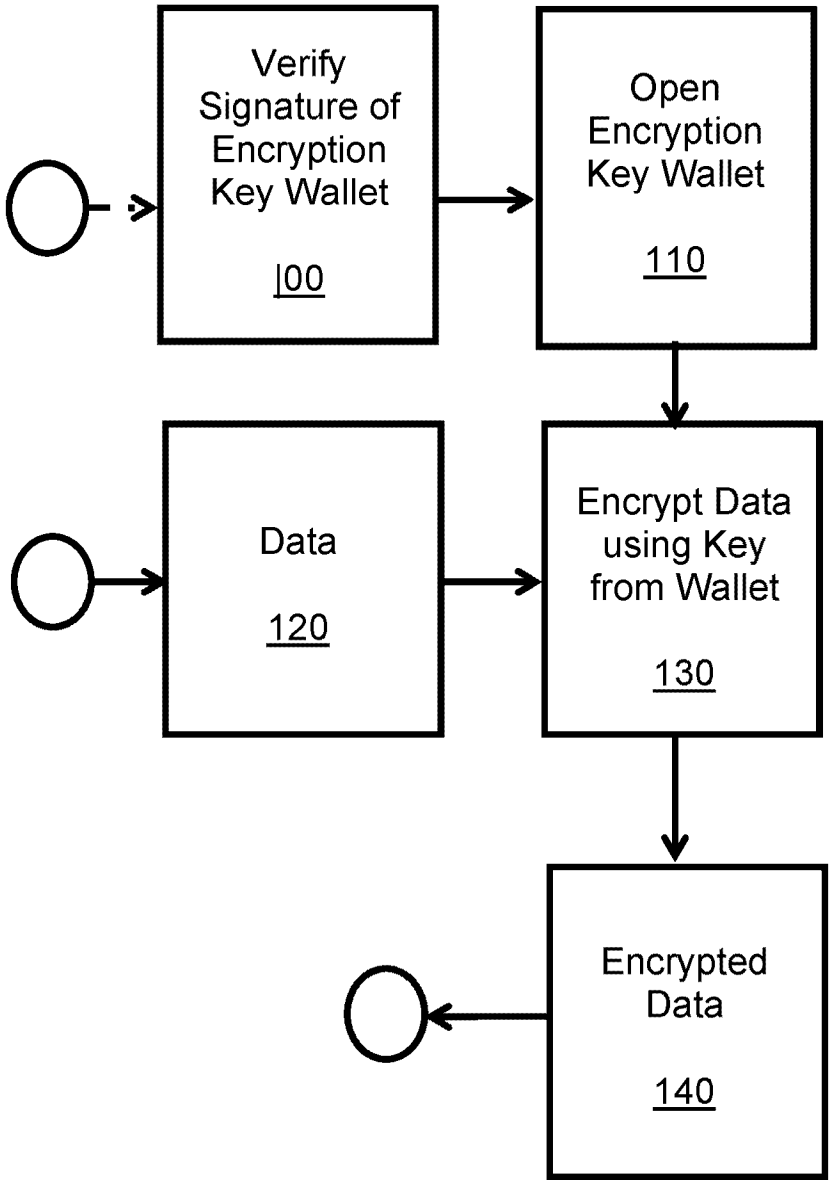
Verify Signature of Encryption Key Wallet
100
Open Encryption Key Wallet
110
Data
120
Encrypt Data using Key from Wallet
130
Encrypted Data
140

FIG. 2a

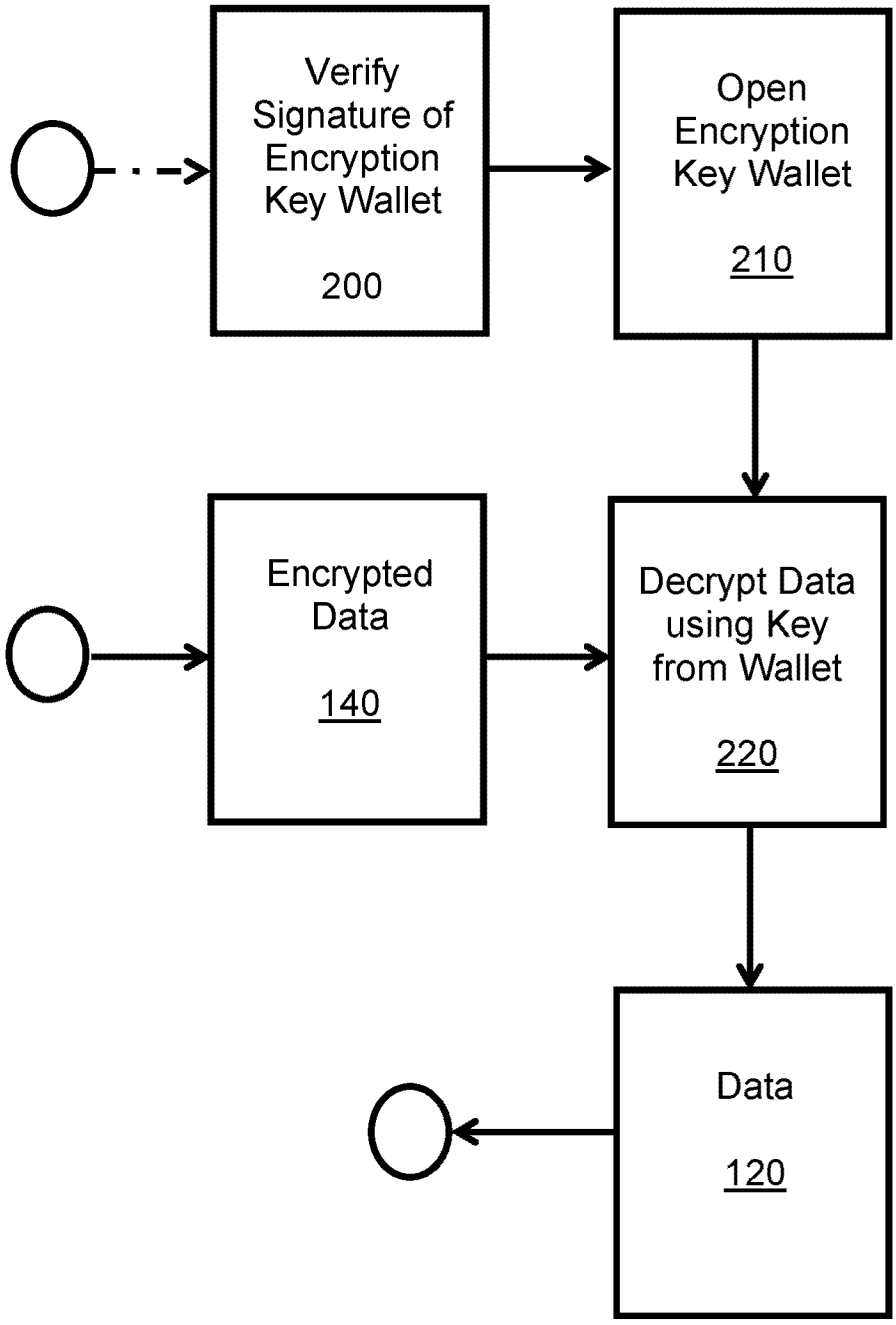
Verify Signature of Encryption Key Wallet
200
Open Encryption Key Wallet
210
Encrypted Data
140
Decrypt Data using Key from Wallet
220
Data
120

FIG. 2b

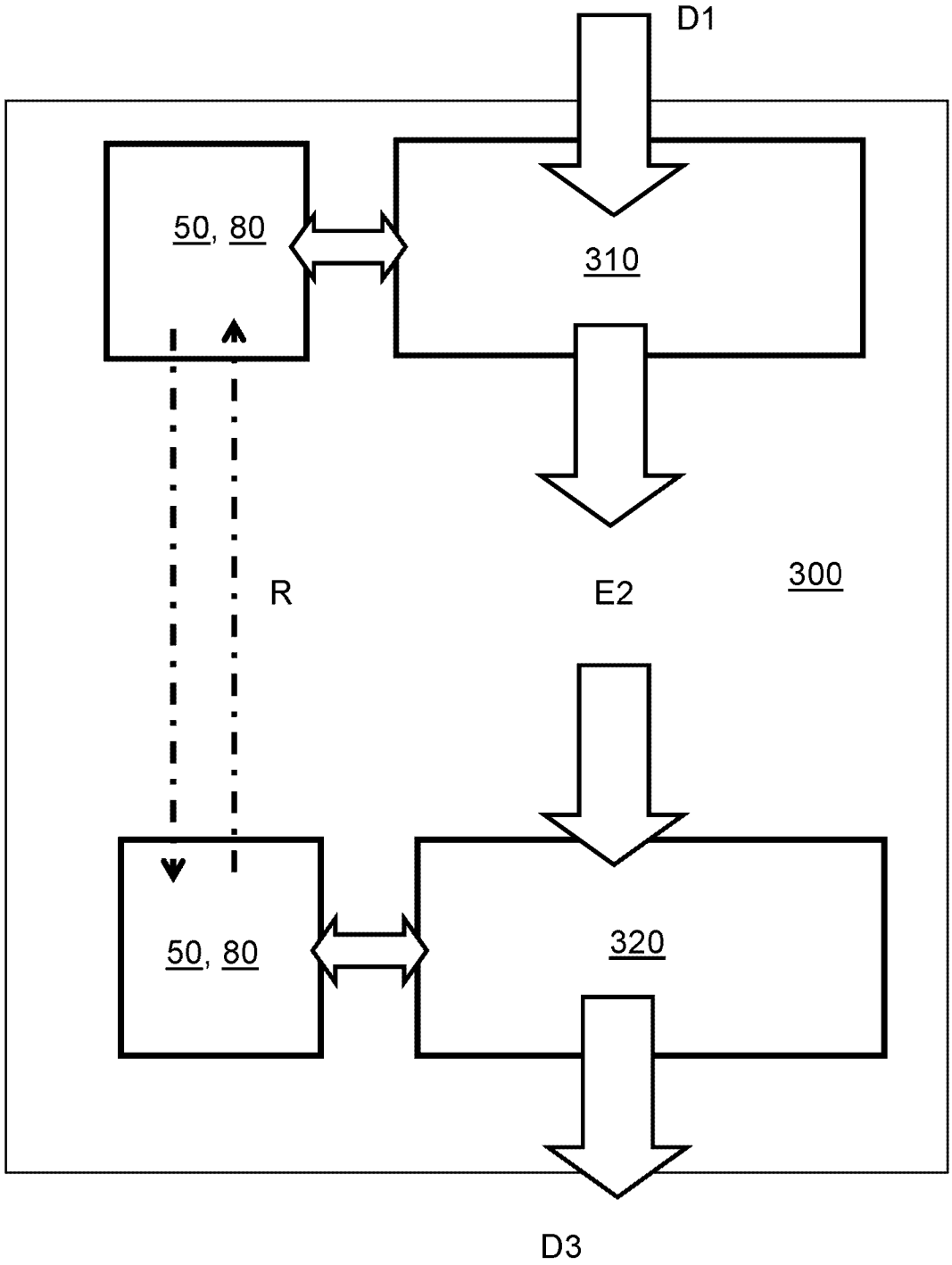

FIG. 3

ENCODER, DECODER, ENCRYPTION SYSTEM, ENCRYPTION KEY WALLET AND METHOD

TECHNICAL FIELD

The present disclosure relates to encoders, corresponding decoders, and encryption systems. Moreover, the present disclosure concerns encryption key wallets for use in aforesaid encryption systems. Furthermore, the present disclosure relates to methods of using aforesaid encryption systems for communicating data in a secure manner. Yet additionally, the present disclosure is concerned with computer program products comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute the aforesaid methods.

BACKGROUND

Encrypting information is necessary in a contemporary information society, both for private citizens as well as for businesses and governmental authorities, because the Internet and other data transfer networks are deeply and permanently integrated into a common infrastructure of the contemporary information society. Therefore, a high degree of reliance is placed on contemporary information systems, and thus data security of reliable information systems is of utmost important and must not be breached. Thus, it is necessary in the aforementioned contemporary information society to encrypt data that are stored and transceived, so that only authorized parties are able to decrypt and read contents of the data.

In known prior art, in order to increase, for example to maximize, security, encryption keys used to encrypt sensitive data are changed frequently for a real-time transfer channel or for information to be transmitted, for example changes to encryption keys are made every few seconds. Resulting newly created

encryption keys are then transmitted with corresponding encrypted information, or alongside it.

During earlier history, various encryption methods for data have been developed along with the development of reading and writing; such encryption methods were mainly used for military purposes. However, especially during the 20th Century, as computers and information networks have become increasingly commonplace, numerous symmetric and asymmetric methods for encrypting data have been developed, of which a most generally known is RSA. RSA (see reference [1]) is a first public key encryption technique. Moreover, RSA was considered to be very strong mathematically, and it initially gave an impression of being unbreakable.

However, later on, when information technology became more commonplace also among regular businesses and average consumers, Pretty Good Privacy (PGP, see reference [2]) was designed. PGP is very well suited for protecting data files, e-mails and hard-disc drives for storing data. It is generally known that the process of encrypting information functions in such a way that either an entire sequence of information, or a part thereof, is encrypted so that only authorized parties can read it. Encryption makes plain text data into encrypted data by utilizing an encryption key, so that the text data can be read by a recipient only if the encrypted data is decrypted with a correct key that an encrypting party involved has given to the recipient.

It is also generally known that, in theory, it is possible to decrypt encrypted data without a key used for generating the encrypted data, but a long encryption key makes it possible to have more permutations, namely function fractional (n!), and thus the longer the key is, the more there arises a need for greater computing capacity to break a given encryption of data, which means that it is practically impossible to break a contemporary well-designed cryptosystem implemented with a strong enough encryption key. However, future increases in computing

power will eventually make even these well-designed cryptosystems vulnerable to hacking and eavesdropping.

One solution to such need has been provided by an encryption key wallet by Oracle Inc. (see ref. [4]). In an arrangement proposed by Oracle Inc., it is specifically encrypted keys that are stored in the encryption key wallet, which requires heavy processing; for example, the encrypted keys need to be decrypted for use. Moreover, such an encryption key wallet is not safe, because data can be used if a given encryption key is decrypted.

The aforementioned encryption key wallet proposed by Oracle Inc., and its associated encryption system, are potentially very impractical in online data transfers, because both users involved have to request and transmit keys from one wallet via a communication network for each connection session. The Oracle system is thus clearly intended to be used in local encryption of database elements. That is, the Oracle system is not intended for data transfers between several parties. Thus, the Oracle system and other approaches using a database include storing encryption keys in their own security module, which again can be accessed by many different software modules via a large number of API's and frameworks. Even if there were, for example, sixty five thousand keys, and they were changed every two seconds, such a situation is still problematic, as aforementioned. In these known arrangements based on a database, the encryption key wallet is situated in a security module and it is shared by several modules. Even though a regular user who performs a database query has no direct access to the wallet itself in these systems, the wallet is still shared in their information system, and it is in practice only as strong to third party attacks as the information system itself, where the encryption module with its encryption key wallet is located.

There is therefore a need for a more secure solution to be used when encrypting the data, which can also be used in data transfers between parties.

SUMMARY

The present disclosure seeks to provide an encryption system that is more secure than known contemporary encryption systems.

Moreover, the present disclosure seeks to provide an encoder for use in the aforementioned system.

Furthermore, the present disclosure seeks to provide a decoder for use in the aforementioned system.

In a first aspect, embodiments of the present disclosure provide an encoder for use in an encryption system for encrypting data to generate corresponding encrypted data, characterized in that:

(i) the encoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the encoder is operable to open the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting the data to generate the corresponding encrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet; and

(iii) the encoder is operable to deliver the reference code of the at least one encryption key along with the corresponding encrypted data.

The present disclosure is of advantage in that the encryption system containing an encoder, *mutatis mutandis* a corresponding decoder, is operable to produce and process encryption keys more efficiently than known encryption systems.

Optionally, for the encoder, the encryption key wallet is implemented in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

Optionally, for the encoder, the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

Optionally, the encoder is operable to permit access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

According to a second aspect, there is provided a method of using an encoder of an encryption system for encrypting data to generate corresponding encrypted data, characterized in that the method includes:

(i) providing the encoder with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) using the encoder to open the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting the data to generate the corresponding encrypted data, and to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet; and

(iii) using the encoder to deliver the reference code of the at least one encryption key along with the corresponding encrypted data.

Optionally, the method includes implementing the encryption key wallet in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

Optionally, the method includes signing the encryption key wallet by using a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

Optionally, the method includes permitting access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

According to a third aspect, there is provided a decoder for use in an encryption system for decrypting encrypted data to generate corresponding decrypted data, characterized in that:

(i) the decoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the decoder is operable to receive a reference code identifying at least one encryption key along with the encrypted data; and

(iii) the decoder is operable to open the encryption key wallet for accessing the at least one encryption key via the ~~its~~ reference code, for decrypting the encrypted data to generate the corresponding decrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet.

Optionally, for the decoder, the encryption key wallet is implemented in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

Optionally, for the decoder, the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

Optionally, the decoder is operable to access one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

According to a fourth aspect, there is provided a method of using a decoder of an encryption system for decrypting encrypted data to generate corresponding decrypted data, characterized in that the method includes:

(i) providing the decoder with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) using the decoder to receive a reference code identifying at least one encryption key along with the encrypted data; and

(iii) using the decoder to open the encryption key wallet for accessing the at least one encryption key via the reference code, for decrypting the encrypted data to generate the corresponding decrypted data, and to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet.

Optionally, the method includes implementing the encryption key wallet in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

Optionally, the method includes signing the encryption key wallet by using a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

Optionally, the method includes accessing one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

According to a fifth aspect, there is provided an encryption system for encrypting data in respect of at least one party, characterized in that:

(i) the at least one party is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code; and

(ii) the encryption key wallet is opened for accessing at least one encryption key via its reference code, for encrypting data to generate corresponding encrypted data and/or for decrypting encrypted data to generate corresponding decrypted data, and is closed when not in use, and wherein the at least one encryption key is generated by the encryption key wallet, wherein the reference code is received at or delivered by the at least one party along with the encrypted data.

Optionally, the encryption system is arranged for enabling exchange of encrypted data via the encryption system between two or more parties, characterized in that:

(i) the two or more parties are provided with the encryption key wallet;

(ii) data exchanged between the two or more parties are encrypted using one or more encryption keys obtained from the encryption key wallet; and

(iii) the encryption key wallet is opened for use when encrypting and/or decrypting the data exchanged between the two or more parties.

Optionally, in the encryption system, the encryption key wallet is implemented in a form of at least one of: data, one or more algorithms.

Optionally, in the encryption system, the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are public-private key pair.

Optionally, the encryption system is operable to permit access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

For example, a company Gurulogic Microsystems Oy has developed an embodiment of the present disclosure, which is referred to as a Gurulogic®

Encryption Key Wallet, which, in operation, is used for creating a truly reliable information system, namely encryption system, thereby improving data security that is feasible to be provided to contemporary society. The encryption keys determined and produced by the Gurulogic® Encryption Key Wallet ensure that undesirable or unknown parties cannot access or hamper a given encryption key being used in communication between authorized parties. Thereby, the Gurulogic® Encryption Key Wallet makes it possible to implement considerably faster and more efficient encryption solutions, yet at least as safe and secure as the known encryption systems, if not even more secure.

According to a sixth aspect, there is provided an encryption key wallet for use with the encryption system pursuant to the fifth aspect, characterized in that the encryption key wallet includes one or more encryption keys which are useable for encrypting data and/or decrypting encrypted data, and are referenced in use by one or more corresponding reference codes; and that the encryption key wallet is operable to be opened for use, and closed when not in use.

Optionally, in respect of the encryption key wallet, the one or more keys of the encryption wallet are signed by a private key of a producing party and/or a user, and the one or more keys are accessible and/or verifiable by using a public key corresponding to the private key, wherein the private key and public key form a private-public key pair.

According to a seventh aspect, there is provided a method of using an encryption system for encrypting data in respect of at least one party, characterized in that the method includes:

(i) providing the at least one party with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code; and

(ii) opening the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting data to generate corresponding encrypted data and/or for decrypting encrypted data to generate

corresponding decrypted data, and closing the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet, wherein the reference code is received at or delivered by the at least one party along with the encrypted data.

Optionally, the method is arranged for enabling exchange of encrypted data via the encryption system between two or more parties, characterized in that the method includes:

(i) providing the two or more parties with an encryption key wallet;

(ii) exchanging data between the two or more parties which is encrypted using one or more encryption keys obtained from the encryption key wallet; and

(iii) opening the encryption key wallet for use when encrypting and/or decrypting the data exchanged between the two or more parties.

Optionally, the method includes implementing the encryption key wallet in a form of at least one of: data, one or more algorithms.

Optionally, in the method, the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are public-private key pair.

Optionally, the method includes operating the encryption system to permit access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

According to an eighth aspect, there is provided a computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing

hardware to execute the aforesaid method pursuant to the second, fourth or seventh aspect.

According to a ninth aspect, there is provided an encryption system including an encoder for encrypting data to generate corresponding encrypted data, characterized in that:

(i) the encoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the encoder is operable to open the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting the data to generate the corresponding encrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet; and.

(iii) the encoder is operable to deliver the reference code of the at least one encryption key along with the corresponding encrypted data.

According to a tenth aspect, there is provided an encryption system including a decoder for decrypting encrypted data to generate corresponding decrypted data, characterized in that:

(i) the decoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the decoder is operable to receive a reference code identifying at least one encryption key along with the encrypted data; and

(iii) the decoder is operable to open the encryption key wallet for accessing the at least one encryption key via the reference code, for decrypting the encrypted data to generate the corresponding decrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet.

Additional aspects, advantages, features and objects of the present disclosure would be made apparent from the drawings and the detailed description of the

illustrative embodiments construed in conjunction with the appended claims that follow.

It will be appreciated that features of the present disclosure are susceptible to being combined in various combinations without departing from the scope of the present disclosure as defined by the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The summary above, as well as the following detailed description of illustrative embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the present disclosure, exemplary constructions of the disclosure are shown in the drawings. However, the present disclosure is not limited to specific methods and apparatus disclosed herein. Moreover, those in the art will understand that the drawings are not to scale. Wherever possible, like elements have been indicated by identical numbers.

Embodiments of the present disclosure will now be described, by way of example only, with reference to the following diagrams wherein:

FIG. 1a is a schematic illustration of a method of creating encryption keys within an encryption system pursuant to the present disclosure;

FIG. 1b is a schematic illustration of a method of storing the encryption keys from FIG. 1a;

FIG. 1c is a schematic illustration of a process of signing encryption keys pursuant to the present disclosure;

FIG. 1d is a schematic illustration of encrypting an encryption key wallet, pursuant to the present disclosure;

FIG. 1e is a schematic illustration of transmitting a secured encryption key wallet, pursuant to the present disclosure;

FIG. 2a is a schematic illustration of encrypting data using the encryption key wallet of FIG. 1e; and

FIG. 2b is a schematic illustration of decryption using the encryption key wallet, wherein there is illustrated a decryption process in a given user's device.

In the accompanying diagrams, an underlined number is employed to represent an item over which the underlined number is positioned or an item to which the underlined number is adjacent. A non-underlined number relates to an item identified by a line linking the non-underlined number to the item. When a number is non-underlined and accompanied by an associated arrow, the non-underlined number is used to identify a general item at which the arrow is pointing.

DETAILED DESCRIPTION OF EMBODIMENTS

The following detailed description illustrates embodiments of the present disclosure and ways in which they can be implemented. Although exemplary modes of carrying out the present disclosure have been disclosed, those skilled in the art would recognize that other embodiments for carrying out or practicing the present disclosure are also possible.

In overview, a Gurulogic® Encryption Key Wallet is a file or a software application which is utilized when producing and storing encryption keys used for executing data encryption; for example the Gurulogic® Encryption Key Wallet is optionally implemented in combination with associated hardware, for example application specific digital circuits such as ASIC's. Optionally, the Gurulogic® Encryption Key Wallet is also used for encrypting information that is being transmitted between two or more parties, for example two or more parties that are mutually coupled together via a data communication network. The encryption keys produced by the Gurulogic® Encryption Key Wallet make it possible for a given data producer to define a secure and very efficient arrangement for protecting all types of digital information, such as data files, e-mails, audio data, image data, video data,

sensor data, biological signal data, genetic readout data, genomic data, forensic data, and so forth. The encryption keys retrieved from the Gurulogic® Encryption Key Wallet do not need to be transmitted between the two or more communicating parties, because the two or more parties using the Encryption Key Wallet know which encryption key has been used to encrypt which particular piece of information, thus establishing a very cost-efficient approach and arrangement for protecting valuable data.

It will be appreciated that the Encryption Key Wallet is also optionally used for encrypting data inside a given device, without any transmission being required with a data producer. In such a case, there is a reference code in the data file and an encryption key in the Encryption Key Wallet. When decrypting the data within the given device, the encryption key according to a next reference code is brought from the Encryption Key Wallet. Thus, the wallet is optionally also utilized at a spatially local level, as one means for encrypting data.

Data encryption systems and associated technology described in the present disclosure makes it possible for a producer of an Encryption Key Wallet to define encryption keys to be produced for the Encryption Key Wallet, and used mutually by two or more communicating parties for data encryption purposes. Optionally, some given producer, for example a service provider, can have a common wallet in use with several consumers and thus, the producer is able to send information simultaneously to many consumers, or else the producer is able to synchronize the number of the used key to inform the users accordingly; in other words, no key needs to be transmitted, but only a reference code of the key to be used, for example when communicating data in a secure manner in embodiments of the present disclosure. Moreover, with the help, for example, of the Gurulogic® Encryption Key Wallet, verification of the data itself or identification of a given data transmitter involved are no longer necessary, and thus a given encryption key being used no longer has to be transmitted with the encrypted data. This is possible, because the encryption keys are previously known to the two or more communicating parties. It will be appreciated that data encryption does not

decrease a payload available for the data to be transmitted, when the encryption methods pursuant to the present disclosure are used; it will be appreciated that even if data compression is not a primary purpose for embodiments of the present disclosure, the embodiments are capable of delivering the same data using less data packets than in known encryption arrangements. For these reasons, the Gurulogic® Encryption Key Wallet enables there to be implemented a considerably simpler and faster cryptography method and arrangement that consumes less energy, as compared with known contemporary methods of encrypting data for communication between two or more mutually communicating parties.

When the Gurulogic® Encryption Key Wallet pursuant to the present disclosure is opened, its digital signature must be verified at all times so that not only the integrity of the content is ensured but also that the content was produced by an authorized party, and that no undesirable or unknown party has tampered with the contents of the Gurulogic® Encryption Key Wallet. Therefore, unlike known contemporary encryption arrangements, the encryption information itself does not need to be digitally signed, when implementing methods pursuant to the present disclosure, because the verification is executed while opening the Gurulogic® Encryption Key Wallet, whereby processing power and time are not wasted unnecessarily when information is being encrypted or decrypted. Such reduction of processing power is especially useful in portable data processing devices, for example smart phones, tablet computers, miniature worn communication devices such as smart watches, and so forth.

Optionally, the Gurulogic® Encryption Key Wallet can remain open during encryption and decryption of data, but it is advantageously closed as soon as its services are no longer required, so that viruses or other malware do not have an opportunity to find out a given encryption key used in encrypting given information. Savings on processing power when methods pursuant to the present disclosure are used are considerable, especially in data transfers where large

amounts of data are processed and transceived, such as in video or genome information communication, for example during forensic investigations.

An important advantage gained by using the methods and arrangements pursuant to the present disclosure is that the data size of the information sequence being encrypted does not grow, since a given encryption key that is employed is not transmitted with the encrypted piece of data. This is a considerable improvement in cases, where data to be encrypted is split into smaller sections without making compromises between data security and the data size being transmitted. Examples of this are, among others, instant messaging, e-mails, DNA data communication, packet data communication, sensor data communication, meta-data communication, and so forth.

Optionally, in addition to being used for encrypting content, the encryption keys of the Gurulogic® Encryption Key Wallet can be used, for example, for encrypting transfer channels, but not limited thereto. The Gurulogic® Encryption Key Wallet can also be used without certificates, when, and if, the verification of the Encryption Key Wallet has been executed in some alternate manner, namely the producer's public key is otherwise verifiable.

The Gurulogic® Encryption Key Wallet can be used cost-efficiently also for protecting a simplex, half-duplex or full-duplex telecommunication connection, where, for example, real-time audio or video streams can be transmitted/received by utilizing encryption keys produced by the Gurulogic® Encryption Key Wallet, thereby not decreasing the payload share available in a given data transfer channel that is employed for communicating the real-time audio or video streams.

The Gurulogic® Encryption Key Wallet superficially resembles a generally known Transaction Authentication Number (TAN) list with which a service provider is able to verify the authenticity of a given person by asking not only the person's user name and pass word, but also Indexed TANs (index-TAN pairs), either regularly or randomly. A hard copy or electronic authentication number list is

strong, because it can be used to verify the authenticity of a person since it is bound to the person's user name. However, it cannot be efficiently used to encrypt information, because an Indexed TAN is usually too short for being used as an encryption key. Moreover, on account of a TAN list being static, it cannot be used in a manner akin to the Gurulogic® Encryption Key Wallet mechanism to produce encryption keys, for example if it is intended that a function be used to produce them.

The Gurulogic® Encryption Key Wallet is not restricted to use of one particular encryption algorithm, and thus the encryption keys produced by it can be used both with symmetric and also with asymmetric encryption algorithms. An example pertains to the aforementioned PGP cryptosystem which encrypts data with a disposable or transient encryption key, namely a "*Session Key*", which is transmitted with the encrypted data, namely asymmetrically encrypted. The Session Key used by PGP can, in its entirety, be replaced by an encryption key produced by the Gurulogic® Encryption Key Wallet, in which case:

(a) the transient session key is not created;

(b) it is not protected by asymmetric cryptography; and

(c) it is not transmitted with the encrypted data.

Encryption methods pursuant to the present disclosure are considerably faster and more cost-efficient to known encryption methods, for example as aforementioned, both as regards computing power and also as regards transfer capacity. The Gurulogic® Encryption Key Wallet defines a mechanism for producing encryption keys which can be used to strengthen an already existing encryption key, or for replacing an encryption key used by a cryptosystem.

By default, as a producer creates or edits an instance of the Gurulogic® Encryption Key Wallet, its contents need to be digitally signed and encrypted using asymmetrical cryptography, with the producer's own private key, against the public keys of other parties involved. This protection of the Gurulogic® Encryption Key Wallet can be implemented for instance by using Public Key Cryptography (PKI, see reference [3]) which achieves a mathematically strongest

possible, namely practically unbreakable, protection, using contemporary computing resources.

The producer's own private key must be stored correctly and encrypted with a symmetric cryptography method, such as contemporary AES. The encrypted private key is opened and decrypted, so that it can be used by entering a passphrase determined by the cryptosystem, or some other type of credential such as a finger print or a biological EKG, for example.

In order to achieve enhanced encryption strength, for example maximal encryption strength, it is recommended in embodiments of the present disclosure to use a pass phrase which consists of a person's individual bio-information, because regular methods cannot be used to break them, unlike usual passwords, thereby making it considerably harder to break them. However, methods of data encryption pursuant to the present disclosure are not limited by:

(a) into which cryptosystem they can be integrated;

(b) which encryption algorithm is used to protect the Gurulogic® Encryption Key Wallet; or

(c) in which way the digital signature has been implemented, because the methods pursuant to the present disclosure focus on defined creation and usage of encryption keys.

In addition to being used in data encryption, the Gurulogic® Encryption Key Wallet can be adapted to be used for any passphrases such as:

(a) a user name of information systems or services, for example with an automatically changing pass phrase;

(b) for PKI key pairs, for example to encrypt a private key symmetrically;

(c) in automated online payments via a bank or a credit card company, for example to verify a payment transaction with a payment identification key stored in the Gurulogic® Encryption Key Wallet;

(d) in traditional card payments, for example a given PIN code or a given CVC code of a credit card are defined in the Gurulogic® Encryption Key Wallet;

(e) for identifying a user with an agreed key pair; and

(f) in entrances to buildings and rooms, for example the Gurulogic® Encryption Key Wallet holds the entrance codes, for example per GPS spatial location.

The Gurulogic® Encryption Key Wallet can also, in certain situations, be protected in a simpler fashion, by using symmetric cryptography, but in such a case, a given producer must either provide a passphrase or credential with each participant, or negotiate a suitable one with them. Such a passphrase is then used to open the Encryption Key Wallet for use.

The Gurulogic® Encryption Key Wallet can also be created and used in an alternative way, namely in an unencrypted manner, if it is not connected with an information system or device executing the encryption. For example, a user can keep an open Gurulogic® Encryption Key Wallet in his or her cellular phone, for example smart phone. A given server or product, or a selected reference code, can then be used to retrieve encryption keys from the Encryption Key Wallet to encrypt or decrypt data; it will be appreciated that the reference code is optionally received also from the server or the cellular phone itself. If the Gurulogic® Encryption Key Wallet has not been protected with asymmetric cryptography, then the digital signature becomes optional, which means that it can only ensure the integrity of the content, but not an intentional change. Therefore, an unprotected digital signature does not prevent undesirable parties or malware from tampering with the contents of the Gurulogic® Encryption Key Wallet.

The functionality of the Gurulogic® Encryption Key Wallet has two phases:

(i) a creation phase at its creation, which is executed only once per Gurulogic® Encryption Key Wallet, and which is described later with reference to FIG.'s 1a, 1b, 1c, 1d, amongst others FIG. 1e; and

(ii) a usage phase, namely for data encryption and decryption, which is described later with reference to FIG.'s 2a and 2b.

Optionally, along with the data encrypted with the Gurulogic® Encryption Key Wallet, the reference code of the encryption key, or some other type of identification, is transmitted with which it is possible to refer to the key pair and which can be used either automatically or manually. The automatic use of the Gurulogic® Encryption Key Wallet is implemented so that, as a user is proceeding to open the Encryption Key Wallet, it is possible to request a specific key pair by using a pre-defined interface.

The automatic use of the Gurulogic® Encryption Key Wallet requires that support for it be implemented in the interface being programmed, so as to enable its encryption function. It will be appreciated that, when the Gurulogic® Encryption Key Wallet is used automatically, the interface is allowed to process only such encryption key pairs that were specifically created or defined for it, so that possible malware or corrupted systems or other malicious parties cannot phish for encryption key pairs that have been intended for other usage scenarios or for other parties.

The Gurulogic® Encryption Key Wallet can also be used manually by a legitimate owner of the Encryption Key Wallet who is allowed and able to open the Encryption Key Wallet for use. Simplest examples of such a scenario are a hard-copy TAN list or a key code list in a Gurulogic® Encryption Key Wallet that may reside, for example, in a given user's smart phone. If the Gurulogic® Encryption Key Wallet resides in a user's personal smart phone, then it can be implemented so that when opening a smart phone that is PIN code-protected, finger-print-protected, and so forth, the Gurulogic® Encryption Key Wallet is also opened, either:

(a) entirely for all key pairs; or

(b) partly, only for some key pairs.

It will be appreciated that delivering the reference code, or some other type of functionally equivalent identification, for the encryption key to be used is only optional. Namely, the wallet itself can also keep track on the reference code of the last used key, respectively the following key to be used, or the wallet can also

randomly choose a reference code of the key and then deliver it along with the encrypted data to the recipient. The keys are not necessary to be used in a specific order, for example they can be selected randomly from a collection of encryption keys. However, as aforementioned, in such a case, the reference code of the key used needs to be delivered along with the data. This decreases the payload; however, a degree of decrease of payload is smaller compared to delivering the encrypted encryption key, due to the length of the reference code being smaller than the length of the encryption key. However, it strengthens the encryption of the data compared to known encryption arrangements, as the information including only the reference code cannot in anyway be used to decrypt the data.

Moreover, opening the Gurulogic® Encryption Key Wallet can also be determined to occur at a certain spatial location or at a certain point in time. In the first case, namely at the certain spatial location, the defined key pairs can be retrieved for use only at a certain geographical location; in such case, the operation protected by the Encryption Key Wallet can be executed only at that certain location. In the latter case, namely at the certain point in time, for example, an automated purchase can be performed only during pre-defined opening hours. Alternatively, in another example case, purchases can be made only in pre-defined shops, or the key pairs needed to open electrical doors and entrance security systems of a user's home can be retrieved from the Encryption Key Wallet, only in an immediate spatial vicinity of the user's home.

To be able to function, the Gurulogic® Encryption Key Wallet requires a device into which it is either embedded as a dedicated microchip, or it is stored as executable software instructions in the memory of the device. Optionally, the Gurulogic® Encryption Key Wallet requires a network connection so that it can access online events. Moreover, optionally, the Gurulogic® Encryption Key Wallet requires access to spatial location data, which access can be implemented with a GPS receiver or an assisted GPS receiver, such an assisted GPS receiver employing spatial location services based on triangulation sensors, with location services based on accelerometers, and so forth.

Occasionally, the Gurulogic® Encryption Key Wallet optionally needs to be able to operate online so that producers can insert new encryption key pairs, edit existing encryption key pairs or delete encryption key pairs. Moreover, via the online access, in case a given device is mislaid or is stolen or abused, the usage of Gurulogic® Encryption Key Wallet can be prevented entirely or partly; furthermore, the producer can terminate the Encryption Key Wallet of the user by removing the user of the Encryption Key Wallet in question from the producer's information system. Moreover, by using spatial location services, it is possible to find the device fast, alternatively yield better protection in cases where the device containing the Encryption Key Wallet in question is lost or stolen; furthermore, the producer can use spatial location data to follow the movements of the device, and based on the location history, the producer can then change verification procedures if necessary, or optionally prevent the Gurulogic® Encryption Key Wallet from being used, if it were selected to set up the Encryption Key Wallet accordingly.

An order number or other ID of an encryption key or a key pair that has been used from the Gurulogic® Encryption Key Wallet can also be transmitted unencrypted, because the encryption key is protected and known only by the communicating parties. Therefore, knowing the reference code of the encryption key does not jeopardize corresponding information which is encrypted using the encryption key. Optionally, in automatic use of the Gurulogic® Encryption Key Wallet, it is possible for the Encryption Key Wallet to request the reference code or other ID of the encryption keys, or key pairs, being used, so that the operation between parties involved in exchanging encrypted data remains synchronous.

The encryption keys produced by the Gurulogic® Encryption Key Wallet are advantageously expanded to comply with a given cryptosystem being used, when necessary. Thus, the Encryption Key Wallet does not impose use of any particular encryption algorithm, and therefore it does not alter or compromise a protection or an execution provided by an encryption method being used in the encryption system. The Gurulogic® Encryption Key Wallet optionally also contains

encryption key pairs that are used as checksums or hashes, or as identifications (ID's). When used in such a manner, it is possible for the Encryption Key Wallet to produce such items and to replace, for example, the use of a random number generator, if certain encryption key pairs are used in place of produced random numbers, for example in a manner akin to a Session Key of the known PGP cryptosystem.

Additionally, the Gurulogic® Encryption Key Wallet is optionally combined with a GMVC® codec which employs technology designed by Gurulogic® Microsystems Oy, thereby enabling yet stronger encryption keys to be the created, namely as described in patent application GB 1414007.3 ("*Encoder, decoder and methods*"), which is hereby incorporated by reference. Integrating the Gurulogic® Encryption Key Wallet with methods described in the aforementioned patent application GB 1414007.3 makes it possible to implement transparently a function which produces an encryption key for a next block of data to be encrypted, thereby preventing malicious parties from reverse engineering such a combined implementation, because a given function that produced the encryption key was retrieved from a protected Gurulogic® Encryption Key Wallet.

It will be appreciated, for the purposes of the present disclosure, an "encoder" as claimed is to be considered as a device, a circuit, a transducer, a software program, an algorithm or a person, or any combination of these, that converts information from one format or code to another, for purposes of standardization, speed, secrecy, security or compressions, for example as defined by Wikipedia link: http://en.wikipedia.org/wiki/Encoder.

Next, example embodiments of the present disclosure will be described in greater detail with reference to FIG. 1a to FIG. 2b.

In FIG. 1a, a producer **10**, represented by a horizontally striated smiley, creates one or more encryption keys **20** to be used, or defines one or more creation methods for creating such encryption key(s). An encryption key may consist of

any bytes, alternatively bits, words, numbers, alphabets, but not limited thereto, and it can have any length. The encryption key can be referred to by employing an order number, denoted by **30**. For example, an encryption key can be generated by using a function f(x), or it can be combined with a previous encryption key.

Referring next to FIG. 1b, the producer **10** stores the one or more encryption keys **20** in a file or software application as an empty wallet **40** to generate a Gurulogic® Encryption Key Wallet **50**.

Referring next to FIG. 1c, the producer **10** then digitally signs the Encryption Key Wallet **50** with his or her private key to generate a corresponding digitally signed Encryption Key Wallet **60**.

Referring next to FIG. 1d, the producer **10**, again represented by a horizontally striated smiley, encrypts the digitally signed Encryption Key Wallet **60** using public keys of both parties, namely the producer **10** and a user **70**, wherein the user **70** is represented by a vertically striated smiley. There is thereby generated a secured Encryption Key Wallet **80**.

Referring next to FIG. 1e, the producer **10** then transmits the secured Encryption Key Wallet **80** to all parties, for example to the producer **10** and to the user **70**, and optionally to other users. Optionally, it is also possible not to transmit the Encryption Key Wallet **80**, but instead, it is pre-installed in a place of business of the producer, for example at a Hesburger® retail store, certain banks, and so forth. In such cases, it is thereby potentially possible to avoid all those risks that relate to transmission of the Encryption Key Wallet **80** via the Internet or similar type of data communication network, for example, even if this is usually a fastest option for communicating the Encryption Key Wallet **80**. Moreover, for example, elderly people potentially may envisage an option of pre-installation as a more convenient way to get the Encryption Key Wallet **80** in use, as they only need to loan their device for a while for installation of the Encryption Key Wallet **80**.

Next, a method of encrypting data will be described, with reference to steps of the method which are represented by rectangular features in FIG. 2a; the method is employed, for example in a device of the user **70**. It is assumed by default that the producer **10** is included amongst communicating parties; however, the producer **10** can also optionally be a third party who assists the parties in creating and using the Gurulogic® Encryption Key Wallet **80**.

In FIG. 2a, in steps **100**, **110**, the parties open the received secured Gurulogic® Encryption Key Wallet **80** by using their own private keys, and then they read or use one of the encryption keys therefrom, which can optionally be expanded if necessary, thereby providing a selected key. The selected key is then used in an encryption step **130** to encrypt data **120** to be transmitted as encrypted data **140**, using a defined symmetric encryption method. A digital signature is not needed, because only the communicating parties know the encryption keys that are employed.

Next, a method of decrypting encrypted data, for example generated pursuant to the method of FIG. 2a, will be described with reference to FIG. 2b; the method of decrypting encrypted data is, for example, executed in the device of the user **70**, or optionally in devices of other users.

In FIG. 2b, steps of the method of decrypting encrypted data are represented by rectangular features. The received encrypted data **140** is decrypted in a decryption step **220** by the method of decrypting encrypted data which corresponds to an inverse of the encryption method described in the foregoing with reference to FIG. 2a. The secure Gurulogic® Encryption Key Wallet **80** is opened in steps **200**, **210** with the user's own private key and by reading or using the referred encryption key, against which the symmetric encryption is decrypted. The encrypted data **140** does not need to be verified, because only the communicating parties can possess and be aware of the used encryption key, whereby not even the identification of the sender needs to be executed, namely

used in the decryption method, to implement a step **220** of decrypting the encrypted data **140** to generate corresponding decrypted data **120**.

Optionally, in FIG. 2a and FIG. 2b, the encryption keys contained in or generated by the Gurulogic® Encryption Key Wallet **60**, **80** can be used to encrypt data between both parties, namely from a given consumer to the producer **10**, or optionally from the producer **10** to the given consumer. It will further be appreciated that the encryption keys, in such a case, either can use the same reference code or beneficially different reference codes can be applied for them, so that they will not be unsynchronized if both parties are simultaneously transmitting new data. More optionally, there could even be different encryption keys for the same reference code, depending on which direction the data is transmitted to in respect of the parties.

The encryption system pursuant to the present disclosure is susceptible to being implemented in a wide variety of devices and apparatus, for example:

(i) smart phones, tablet computers, personal computers, laptop computers, wearable electronic devices;

(ii) video conferencing systems, security systems, electrical smart grid, medical equipment and apparatus, music delivery system, video delivery systems, telephony systems, financial transaction systems, data communication systems, financial share dealing systems, hedge-fund trading systems, financial derivatives trading platform systems, the Internet, air traffic control systems, geological surveying equipment and apparatus, genomic readout (DNA or RNA readout) equipment and apparatus, video and/or audio distribution systems, video and/or audio replaying devices,

but not limited thereto.

The encryption system pursuant to the present disclosure is highly desirable for situations wherein data of a confidential or sensitive nature is to be exchanged securely between a plurality of parties to the encryption system, wherein it is feasible to communicate encryption key wallet information a priori between the

parties before encrypted data is exchanged, or via an independent communication path to that employed for the encrypted data. For example, the encryption key wallet is optionally implemented as a contemporary USB dongle which can be inserted into USB sockets of tablet computers, laptop computers, personal computers and similar. However, the encryption key wallet is susceptible to being communicated as a data file between the parties to the encryption system. Other implementations of the encryption system are possible pursuant to the present disclosure.

It will be appreciated that embodiments of the present disclosure are optionally implemented using computing hardware which is operable to execute program instructions for implementing methods pursuant to the present disclosure. Alternatively, embodiments of the present disclosure can be implemented, at least in part, in dedicated digital hardware, for example via use of application-specific integrated circuits (ASIC's).

In the foregoing, with regard to the Encryption Key Wallet **80**, it will be appreciated that a given reference code can be employed to define a corresponding encryption key in the Encryption Key Wallet **80**, and it is the given reference code that is optionally communicated between parties involved when communicating encrypted data therebetween; the parties are provided, for example, *a priori* with the Encryption key wallet **80**. Such an implementation is a single level mapping from the reference code to its corresponding encryption key. However, optionally, it will be appreciated that multiple layers of reference codes can be employed. For example, a first tier reference code communicated between the parties is used to reference a look-up table communicated between the parties *a priori* to find a second tier reference code which is used to access an encryption key within the Encryption key wallet **80**. Optionally, several layers of look-up table are employed; for example, a first tier reference code references a second tier reference code via a first look-up table, and the second tier reference code references a third tier reference code via a second look-up table, wherein the third tier reference code is used to access a relevant corresponding encryption

key from the Encryption key wallet **80** for use in decrypting encrypted data. Optionally, the look-up tables are stored at a remote server which is accessible to a plurality of decoders, for example in a multicasting situation; in such a situation, access to the look-up tables stored at the remote server allow control of access to data, for example in a situation of release of a new video production via multicasting to a multitude of mutually spatially dispersed decoders.

Modifications to embodiments of the present disclosure described in the foregoing are possible without departing from the scope of the present disclosure as defined by the accompanying claims. Expressions such as "including", "comprising", "incorporating", "consisting of", "have", "is" used to describe and claim embodiments of the present disclosure are intended to be construed in a non-exclusive manner, namely allowing for items, components or elements not explicitly described also to be present. Reference to the singular is also to be construed to relate to the plural. Numerals included within parentheses in the accompanying claims are intended to assist understanding of the claims and should not be construed in any way to limit subject matter claimed by these claims.

REFERENCES

[1] RSA (cryptosystem) - Wikipedia, the free encyclopedia (accessed March 5, 2015). URL: http://en.wikipedia.org/wiki/RSA_%28cryptosystem%

[2] Pretty Good Privacy - Wikipedia, the free encyclopedia (accessed March 5, 2015). URL: http://en.wikipedia.org/wiki/Pretty_Good_Privacy

[3] Public-key cryptography - Wikipedia, the free encyclopedia (accessed March 5, 2015). URL: http://en.wikipedia.org/wiki/Public-key_cryptography

[4] Oracle Encryption Wallet. URL: http://docs.oracle.com/cd/B19306_01/network.102/b14268/asotrans.htm#ASOAG600

CLAIMS

We claim:

1. An encoder for use in an encryption system for encrypting data to generate corresponding encrypted data, characterized in that:

(i) the encoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the encoder is operable to open the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting the data to generate the corresponding encrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet; and

(iii) the encoder is operable to deliver the reference code of the at least one encryption key along with the corresponding encrypted data.

2. The encoder of claim 1, characterized in that the encryption key wallet is implemented in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

3. The encoder of claim 1 or 2, characterized in that the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

4. The encoder of claim 1, 2 or 3, characterized in that the encoder is operable to permit access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

5. A method of using an encoder of an encryption system for encrypting data to generate corresponding encrypted data, characterized in that the method includes:

(i) providing the encoder with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) using the encoder to open the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting the data to generate the corresponding encrypted data, and to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet; and

(iii) using the encoder to deliver the reference code of the at least one encryption key along with the corresponding encrypted data.

6. The method of claim 5, characterized in that the method includes implementing the encryption key wallet in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

7. The method of claim 5 or 6, characterized in that the method includes signing the encryption key wallet by using a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

8. The method of claim 5, 6 or 7, characterized in that the method includes permitting access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

9. A decoder for use in an encryption system for decrypting encrypted data to generate corresponding decrypted data, characterized in that:

(i) the decoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the decoder is operable to receive a reference code identifying at least one encryption key along with the encrypted data; and

(iii) the decoder is operable to open the encryption key wallet for accessing the at least one encryption key via the reference code, for decrypting the encrypted data to generate the corresponding decrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet.

10. The decoder of claim 9, characterized in that the encryption key wallet is implemented in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

11. The decoder of claim 9 or 10, characterized in that the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

12. The decoder of claim 9, 10 or 11, characterized in that the decoder is operable to access one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

13. A method of using a decoder of an encryption system for decrypting encrypted data to generate corresponding decrypted data, characterized in that the method includes:

(i) providing the decoder with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) using the decoder to receive a reference code identifying at least one encryption key along with the encrypted data; and

(iii) using the decoder to open the encryption key wallet for accessing the at least one encryption key via the ~~its~~ reference code, for decrypting the encrypted data to generate the corresponding decrypted data, and to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet.

14. The method of claim 13, characterized in that the method includes implementing the encryption key wallet in a form of at least one of: data, one or more algorithms, hardware, a micro circuit.

15. The method of claim 13 or 14, characterized in that the method includes signing the encryption key wallet by using a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

16. The method of claim 13, 14 or 15, characterized in that the method includes accessing one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

17. An encryption system for encrypting data in respect of at least one party, characterized in that:

(i) the at least one party is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code; and

(ii) the encryption key wallet is opened for accessing at least one encryption key via its reference code, for encrypting data to generate corresponding encrypted data and/or for decrypting encrypted data to generate corresponding decrypted data , and is closed when not in use, and wherein the at least one encryption key is generated by the encryption key wallet, wherein the reference code is received at or delivered by the at least one party along with the encrypted data.

18. An encryption system of claim 17, for enabling exchange of encrypted data via the encryption system between two or more parties, characterized in that:

(i) the two or more parties are provided with the encryption key wallet;

(ii) data exchanged between the two or more parties are encrypted using one or more encryption keys obtained from the encryption key wallet; and

(iii) the encryption key wallet is opened for use when encrypting and/or decrypting the data exchanged between the two or more parties.

19. The encryption system of claim 17 or 18, characterized in that the encryption key wallet is implemented in a form of at least one of: data, one or more algorithms, hardware, micro circuit.

20. The encryption system of claim 17, 18 or 19, characterized in that the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair.

21. The encryption system of claim 18, characterized in that the encryption system is operable to permit access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

22. An encryption key wallet (80) for use with the encryption system of claim 17, characterized in that:

(i) the encryption key wallet includes one or more encryption keys which are useable for encrypting data and/or decrypting encrypted data, and are referenced in use by one or more corresponding reference codes; and

(ii) the encryption key wallet is operable to be opened for use, and closed when not in use.

23. The encryption key wallet (80) of claim 22, characterized in that the one or more keys of the encryption wallet are signed by a private key of a producing party and/or a user, and the one or more keys are accessible and/or verifiable by using a public key corresponding to the private key, wherein the private key and public key form a private-public key pair.

24. A method of using an encryption system for encrypting data in respect of at least one party, characterized in that the method includes:

(i) providing the at least one party with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code; and

(ii) opening the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting data to generate corresponding encrypted data and/or for decrypting encrypted data to generate corresponding decrypted data, and closing the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet, wherein the reference code is received at or delivered by the at least one party along with the encrypted data.

25. The method of claim 24, for enabling exchange of encrypted data via the encryption system between two or more parties, characterized in that the method includes:

(i) providing the two or more parties with the encryption key wallet;

(ii) exchanging data between the two or more parties which is encrypted using one or more encryption keys obtained from the encryption key wallet; and

(iii) opening the encryption key wallet for use when encrypting and/or decrypting the data exchanged between the two or more parties.

26. The method of claim 24 or 25, characterized in that the method includes implementing the encryption key wallet in a form of at least one of: data, one or more algorithms.

27. The method of claim 25 or 26, characterized in that the encryption key wallet is signed by a private key of a producer of data and/or a transmitter of data, and the encryption key wallet is verifiable by using a public key associated with the private key, wherein the public key and private key are a public-private key pair,

28. The method of claim 25, 26 or 27, characterized in that the method includes operating the encryption system to permit access to one or more keys of the encryption wallet depending upon at least one of:

(i) a spatial and/or geographical location of a recipient party; and

(ii) a temporal instant of the recipient party.

29. A computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute a method as claimed in claim 5, 13 or 24.

30. An encryption system including an encoder for encrypting data to generate corresponding encrypted data, characterized in that:

(i) the encoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the encoder is operable to open the encryption key wallet for accessing at least one encryption key via its reference code, for encrypting the data to generate the corresponding encrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet; and.

(iii) the encoder is operable to deliver the reference code of the at least one encryption key along with the corresponding encrypted data.

31. An encryption system including a decoder for decrypting encrypted data to generate corresponding decrypted data, characterized in that:

(i) the decoder is provided with an encryption key wallet, wherein one or more encryption keys of the encryption key wallet are identifiable using at least one reference code;

(ii) the decoder is operable to receive a reference code identifying at least one encryption key along with the encrypted data; and

(iii) the decoder is operable to open the encryption key wallet for accessing the at least one encryption key via the reference code, for decrypting the encrypted data to generate the corresponding decrypted data, and is operable to close the encryption key wallet when not in use, and wherein the at least one encryption key is generated by the encryption key wallet.