ALLNAMES:(PQ Solutions Limited)

17 results Offices all Languages en Stemming true Single Family Member false Include NPL false

Sort: Relevance Per page: 200 View: All 1 / 1 Machine translation

1. **20150326510** METHOD AND APPARATUS FOR TIME LIMITED MESSAGES IN PACKET COMMUNICATIONS — US - 12.11.2015

Int.Class H04L 12/58 **Appl.No** 14306515 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Systems and methods are provided for direct packet communications and store and forward packet communications including packets which have attributes which determine the lifetime of the packet contents and these lifetimes are optionally a function of the recipient. Example methods are given featuring the transmission of packets with limited lifetime, the storing and retransmission of packets to one or more recipients and confirmation of deletion of packet contents. It is also shown that cryptography may be employed to ensure that timed presentation of packet contents to recipients takes place and is authenticated by the sender.

2. **20180054316** MULTIPLE SECRETS IN QUORUM BASED DATA PROCESSING — US - 22.02.2018

Int.Class G06F 21/00 **Appl.No** 15467815 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Methods are described for constructing a secret key by multiple participants such that any quorum combination of participants can generate a fixed number of key components that can be combined by a recipient to generate the secret key. The methods permit an identical secret key to be generated by a different sized quorum from different participants if required. The keys may be used as private keys for encryption, decryption, digital signatures or authentication tokens and each key is generated from a key index. The circuits used by a quorum of participants for the generation of keys feature nested non-linear devices connected in series with outputs multiplied by stored secret values. Example applications are described including blinded cipher text generation, a multi-signature cryptocurrency system and an encrypted cloud storage system.

3. **20160191513** BINDING A DATA TRANSACTION TO A PERSON'S IDENTITY USING BIOMETRICS — US - 30.06.2016

Int.Class H04L 29/06 **Appl.No** 14804010 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Methods and systems are described for binding a data transaction to a person's identity using biometrics. The method comprises the generation of data which includes information associated with a transaction, or an encrypted transaction, between a server and a client device associated with a user, generating authentication data providing an irrevocable binding of the information to biometric characteristics of the user, by capturing biometric input by the user of said authentication data or information associated with the transaction, wherein this information is implanted into the captured data. A predetermined minimum number of quorum portions may be generated from a portion of the data generated or processed by the method, wherein at least a predetermined minimum number of received quorum data portions are required to reconstruct the data portion.

4. **20180225175** CONTROLLED AND VERIFIABLE INFORMATION DESTRUCTION — US - 09.08.2018

Int.Class G06F 11/00 **Appl.No** 15782193 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Digital data archival methods and systems are described, providing controlled and verifiable information destruction. In one embodiment, the method comprises storing digitally encoded information, wherein the information is encoded as a sequence of numbers or symbols using parameters defining an associated error correction ability of an error correcting algorithm based on a lifetime of the digitally encoded information. Errors are periodically added to the sequence of numbers or symbols, such that the digitally encoded information is recoverable from the sequence of numbers or symbols during the defined lifetime, and after a total of number of added errors exceeds the associated error correction ability, the digitally encoded information cannot be retrieved.

5. **20180205536** STREAM CIPHER SYSTEM — US - 19.07.2018

Int.Class H04L 9/06 **Appl.No** 15711361 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

A cipher encryption system and method, where the ciphertext that is produced has two parts, the first part being the result of encrypting a function output of the message by using a block or stream cipher. The message function may be a cryptographic hash of the message. The second part is produced by adding the keystream output of a cryptographic random number generator to the message stream. The seed of the random number generator is determined by combining the encryption key with the hash of the message. Decryption is the reverse process; the message hash is determined by decrypting the first part of the ciphertext and an identical keystream is produced by seeding a cryptographic random number generator with a combination of the encryption key and the decrypted message hash. A method and system are described which produces a keystream with higher entropy than the message, by periodically reseeding the random number generator from hashes of permuted subsets of the message stream that have already been encrypted.

6. **20180262456** METHOD AND APPARATUS FOR TIME LIMITED MESSAGES IN PACKET COMMUNICATIONS — US - 13.09.2018

Int.Class H04L 12/58 **Appl.No** 15980019 **Applicant** PQ SOLUTIONS LIMITED **Inventor** Martin Tomlinson

Systems and methods for direct packet communications and store and forward packet communications are provided that include packets which have attributes which determine the lifetime of the packet contents and these lifetimes are optionally a function of the recipient. Example methods are given featuring the transmission of packets with limited lifetime, the storing and retransmission of packets to one or more recipients and confirmation of deletion of packet contents. It is also shown that cryptography may be employed to ensure that timed presentation of packet contents to recipients takes place and is authenticated by the sender.

7. **20210099290** CIPHERTEXT BASED QUORUM CRYPTOSYSTEM — US - 01.04.2021

Int.Class H04L 29/06 **Appl.No** 16588139 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Methods are described for constructing a secret key by multiple participants from multiple ciphertexts such that any quorum combination of participants can decrypt their respective ciphertexts and so generate a fixed number of key fragments that can be combined by a recipient to generate the secret key. Worked examples are described showing how the encryption keys for the ciphertexts may be key wrapped using a key encapsulation mechanism for which ciphers that are resistant to attack by a quantum computer may be used. In these cases, a post-quantum quorum system is realised. Methods are described by which the quorum key fragment ciphertexts may be updated so that the original key fragments become invalid without necessitating any change to the secret key.

8. **WO/2021/048549** DATA COMMUNICATION BETWEEN A GROUP OF USERS — WO - 18.03.2021

Int.Class H04L 9/32 **Appl.No** PCT/GB2020/052181 **Applicant** PQ SOLUTIONS LIMITED **Inventor** TOMLINSON, Martin

Systems and methods are described for implementing communication of data between a group of users in a communication system. In one implementation, a plurality of quorum portions of a private group signing key are generated and provided to each of a plurality of devices of the group of users, wherein a group digital signature is reconstructed from a predetermined minimum number of encrypted portions of the group digital signature, each generated by a respective device of the group of users using a corresponding quorum portion of the private group signing key. Each user device may digitally sign group output data using a respective private group signing key portion. A reconstructed group digital signature may be verified using a corresponding public group signing key. Other embodiments are also described and claimed.

9. **20200104572** BINDING DATA TO A PERSON'S IDENTITY — US - 02.04.2020

Int.Class G06F 21/32 **Appl.No** 16599497 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Methods and systems are described for creating irrefutable binding data for a data file. An input sequence of data elements is derived based on information from the data file. A graphical representation of input regions corresponding to the input sequence of data elements is output on a display, superimposed on captured image data including a visible feature of a user associated with the data file. User input of each data element of the input sequence is captured by tracking the visible feature through the corresponding input regions, and the binding data is created from the captured images as the visible feature is tracked through the input regions.

10. **20180247111** BINDING DATA TO A PERSON'S IDENTITY — US - 30.08.2018

Int.Class G06F 21/32 **Appl.No** 15711311 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Methods and systems are described for creating irrefutable binding data for a data file. An input sequence of data elements is derived based on information from the data file. A graphical representation of input regions corresponding to the input sequence of data elements is output on a display, superimposed on captured image data including a visible feature of a user associated with the data file. User input of each data element of the input sequence is captured by tracking the visible feature through the corresponding input regions, and the binding data is created from the captured images as the visible feature is tracked through the input regions.

11. **20170324554** PUBLIC KEY CRYPTOSYSTEM BASED ON PARTITIONING OF GALOIS FIELD ELEMENTS — US - 09.11.2017

Int.Class H04L 9/08 **Appl.No** 15587910 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

A post-quantum, public key cryptosystem is described which is polynomial based and where the private key polynomial has coefficients from a sub-set of Galois field elements and plain text message polynomials have coefficients from a second sub-set of Galois field elements. The public key polynomial is constructed using the inverse of the private key polynomial and a randomly chosen polynomial having coefficients chosen from a third sub-set of Galois field elements. Cipher texts are constructed using the public key and randomly chosen session key polynomials. Other more complicated embodiments are described. For implementation a small prime base field such as 2, 3 or 5 will usually be used in constructing the prime power Galois field. The system has the advantage of relatively small public key sizes.

12. **20200301793** SYSTEMS AND METHODS FOR QUORUM-BASED DATA PROCESSING — US - 24.09.2020

Int.Class G06F 11/14 **Appl.No** 16893937 **Applicant** PQ SOLUTIONS LIMITED **Inventor** Martin TOMLINSON

The present disclosure includes systems and methods for quorum-based data processing, in which quorum portions are distributed to candidate participants in determined proportions that control groups of required participants. In exemplary embodiments, a server generates a plurality of quorum portions from original data, wherein the original data includes secret information for data processing within a secured computing environment, and wherein at least a predetermined minimum number of the quorum portions are required to reconstruct the original data. Sets of quorum portions are determined from said plurality of quorum portions, wherein each set includes a respective proportion of the plurality of quorum portions, and at least one set includes a larger proportion of the quorum portions. Each set of quorum portions is distributed to a respective one of a plurality of computing devices associated with respective participants over a data network within a secured computing environment.

13. **20200119923** DATA VERIFICATION — US - 16.04.2020

Int.Class H04L 29/06 **Appl.No** 16658227 **Applicant** PQ Solutions Limited **Inventor** Martin Tomlinson

Systems and methods for user identity and transaction authentication are described. A user may be authenticated by a terminal configured to process image data of a two-dimensional code to decode key information, the two-dimensional code comprising a cryptographic binding of user credentials including a low-resolution image of the user's face and optionally user biometric data to database user information stored on a secure server. A hash of the two-dimensional code has several digits in common with the hash of the user information stored on the secure server. Authentication may be carried out by computing and comparing the hash values, comparing the high-resolution image of the user's face fetched from the secure server to the user and to the low resolution image embedded in the two dimensional code. The two-dimensional code may be generated to provide access to a restricted area.

14. **20180331833** DATA VERIFICATION — US - 15.11.2018

Int.Class H04L 9/32 **Appl.No** 15729880 **Applicant** PQ Solutions Limited **Inventor** Cen Jung Tjhai

Systems and methods for user identity and transaction authentication are described. A user may be authenticated by a terminal configured to process image data of a two-dimensional code to decode key information, the two-dimensional code comprising a cryptographic binding of user credentials including a low-resolution image of the user's face and optionally user biometric data to database user information stored on a secure server. A hash of the two-dimensional code has several digits in common with the hash of the user information stored on the secure server. Authentication may be carried out by computing and comparing the hash values, comparing the high-resolution image of the user's face fetched from the secure server to the user and to the low resolution image embedded in the two dimensional code. The two-dimensional code may be generated to provide access to a restricted area.

15. **WO/2018/206912** DATA VERIFICATION WO - 15.11.2018

Int.Class H04L 29/06 **Appl.No** PCT/GB2018/051088 **Applicant** PQ SOLUTIONS LIMITED **Inventor** TOMLINSON, Martin

Systems and methods for user identity and transaction authentication are described. In one embodiment, a user is authenticated by a terminal configured to process image data of a two-dimensional code to decode key information, the two-dimensional code comprising a cryptographic binding of user credentials including a low-resolution image of the user's face and optionally user biometric data to database user information stored on a secure server. It is arranged that the hash of the two-dimensional code has several digits in common with the hash of the user information stored on the secure server. Authentication is carried out by computing and comparing the hash values, comparing the high-resolution image of the user's face fetched from the secure server to the user and to the low resolution image embedded in the two dimensional code. In other embodiments the two-dimensional code is generated on a user's device as proof of a transaction and may be used subsequently as an admission ticket or as output of a commercial contract.

16. **20190114233** SYSTEMS AND METHODS FOR QUORUM-BASED DATA RECOVERY US - 18.04.2019

Int.Class H04L 9/38 **Appl.No** 16211857 **Applicant** PQ SOLUTIONS LIMITED **Inventor** Martin Tomlinson

The present disclosure includes systems and methods for quorum-based data recovery, in which data is recovered provided at least a minimum number of quorum data portions are presented. In exemplary embodiments, a predetermined minimum number of versions of original data is received, and the original data is reconstructed from the received versions, wherein the original data cannot be reconstructed without loss unless a predetermined minimum number of versions is received. In other embodiments, erroneous or corrupted quorum data portions are detected and associated participants presenting said erroneous or corrupted quorum data portions are identified.

17. **20150378842** SYSTEMS AND METHODS FOR QUORUM-BASED DATA RECOVERY US - 31.12.2015

Int.Class H04L 9/00 **Appl.No** 14683379 **Applicant** Martin Tomlinson **Inventor** Martin Tomlinson

The present disclosure includes systems and methods for quorum-based data recovery, in which data is recovered provided at least a minimum number of quorum data portions are presented. In exemplary embodiments, a predetermined minimum number of versions of original data is received, and the original data is reconstructed from the received versions, wherein the original data cannot be reconstructed without loss unless a predetermined minimum number of versions is received. In other embodiments, erroneous or corrupted quorum data portions are detected and associated participants presenting said erroneous or corrupted quorum data portions are identified.