The creation method of public key encryption and key signature, equipment and readable storage medium storing program for executing

Abstract

The invention discloses a kind of public key encryption for block chain and the creation methods of key signature, it include: step S101, constructor, to meet the encryption data under public key, the side for possessing converter creates message, it could only be decrypted, can only be decrypted using the corresponding privacy key obtained cannot be calculated from public key using the addressee of public key, to realize the public key encryption creation of block chain； Step S102, it selects to create different secret values from the public key encryption of block chain is realized, it is shared for all converters, its other party can not be known, by Hash operation and verification step, verifies agency and check whether signature format is correct and/or whether signs equal to another signature known otherwise.Also disclose corresponding equipment and readable storage medium storing program for executing, the technical solution of the disclosure only uses symmetric cryptography and hash function safely exchanges key, it is proved to create the password of authenticity, integrality and non-repudiation in a manner of basic and is effective, it can not reverse-engineering.

CN109274502A

China

Download PDF Find Prior Art Similar

Other languages: Chinese

Inventor: 安德鲁.威廉.罗斯科, 陈邦道

Worldwide applications

2018 • CN

Application CN201811300417.4A events

2018-11-02 • Application filed by 克洛斯比尔有限公司

2018-11-02 • Priority to CN201811300417.4A

2019-01-25 • Publication of CN109274502A

Info: Legal events, Similar documents, Priority and Related Applications

External links: Espacenet, Global Dossier, Discuss

Claims (23)

Hide Dependent

1. a kind of for the public key encryption of block chain and the creation method of key signature, characterized by comprising:

Step S101, constructor, to meet the encryption data under public key, the side for possessing converter creates message, only The corresponding addressee of used public key could decrypt, and can only be solved using that cannot calculate the corresponding privacy key that obtain from public key It is close, to realize the public key encryption creation of block chain；

Step S102 selects to create different secret values from the public key encryption of block chain is realized, shared for all converters, other Fang Wufa is known, by Hash operation and verification step, verifying agency checks whether signature format is correct and/or whether signs Equal to another signature known otherwise.

2. according to claim 1 for the public key encryption of block chain and the creation method of key signature, it is characterised in that: The function is supplied to user as integrated package, and refusal attacker gets around the chance for decomposing the function, and by institute The a part for stating public key retains secret value in the integrated package, so that the public key can not be from rebuilding.

3. according to claim 1 for the public key encryption of block chain and the creation method of key signature, it is characterised in that: A variety of secure key negotiation methods are carried out using converter, the secure key negotiation method uses self-generating entropy method or dependence The method of user's formation entropy, the method by user's formation entropy include carrying out Hash operation to entropy to prevent third side from attacking It hits.

4. according to claim 3 for the public key encryption of block chain and the creation method of key signature, it is characterised in that: For the agreement finally developed, self-generating entropy method and the method for relying on user's formation entropy include: to breathe out to entropy Uncommon operation prevents the attack of third side.

5. according to claim 1 for the public key encryption of block chain and the creation method of key signature, it is characterised in that The step S101 includes: the user A and B for attempting to agree to key, they respectively possess converter, by A when transmitting starts Negotiation signal is issued to B, B generates secret number N at random in real time$_B$Afterwards to N_BIt carries out Hash operation and obtains hash (N_B), and send A to； A generates X and carries out computations V=enc (hash (mk, hash (N using converter$_B$)),hash(X))； A transmits V value To B, B is by V value and N_BValue is input to converter, and converter, which is decrypted, calculates dec (hash (mk, hash (N_B)), V), it calculates As a result it should be equal to hash (X), A and B by agreeing to hash (hash (X)) finally to confirm the key on public credit channel Hash hash (X), wherein mk is the master key that all converters all know, any other people can not know the master key, enc It is the encryption and decryption function that symmetric key is used in converter with dec.

6. according to claim 5 for the public key encryption of block chain and the creation method of key signature, it is characterised in that: All communications including the final confirmation can be completed on Dolev-Yao network.

7. according to claim 1 for the public key encryption of block chain and the creation method of key signature, it is characterised in that: The converter has the function of

compound function needed for calculating A and B.

8. according to claim 5 for the public key encryption of block chain and the creation method of key signature, it is characterised in that: B is by hash (N_B) it is re-used as disposable or nonexpondable public key, if B is in same type exchange by hash (N_B) it is used as one Secondary or nonexpondable public key, without making change to function, so that it may obtain privacy key N_B。

9. according to claim 1 for the public key encryption of block chain and the creation method of key signature, it is characterised in that The step S102 includes: to input X and private key sk for the X that signs and export enc (hash (ms, hash (sk)), X)； Pass through public affairs The step of key pk is verified, the verifying includes: input Y and pk, is exported dec (hash (ms, pk), Y).Verifying agency checks Whether the format of the signature X is correct and/or the signature X is equal to the signature X known otherwise； Ms is another institute There is the key that converter all knows, other people can not know the master key, and ms must be different from master key mk, enc and dec For the encryption and decryption function for being used for symmetric key in converter.

10. according to claim 9 for the public key encryption of block chain and the creation method of key signature, feature exist It is also used to crack encryption in the step of: verifying.

11. it is any described for the public key encryption of block chain and the creation method of key signature according to claim 5 or 9, It is characterized in that: symmetric cryptography can be used the function f for being easy to calculate, so that dec (k) and enc (f (k)) are identical, remove Non- f be immobilize or comprising a large amount of k in the case where, otherwise can eliminate the angle-of-attack using Hash operation.

12. a kind of for the public key encryption of block chain and the creation equipment of key signature, it is characterised in that: including processor, Described in processor can be used for:

Constructor, to meet the encryption data under public key, the side for possessing converter creates message, is only used public key Corresponding addressee could decrypt, and can only be decrypted using that cannot calculate the corresponding privacy key obtained from public key, to realize The public key encryption of block chain creates；

It selects to create different secret values from the public key encryption of block chain is realized, shared for all converters, other party can not obtain Know, by Hash operation and verification step, whether verifying agency, which checks whether signature format is correct and/or sign to be equal to, passes through Another signature that other way is known.

13. according to claim 12 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: the function is supplied to user as integrated package, and refusal attacker gets around the chance for decomposing the function, and will A part of the public key retains the secret value in the integrated package, so that the public key can not be from reconstruction.

14. according to claim 12 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: carry out a variety of secure key negotiation methods using converter, the secure key negotiation method using self-generating entropy method or By the method for user's formation entropy, the method by user's formation entropy includes carrying out Hash operation to entropy to prevent third side's Attack.

15. according to claim 14 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: for the agreement finally developed, self-generating entropy method and the method by user's formation entropy include: to carry out to entropy Hash operation prevents the attack of third side.

16. according to claim 12 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: the function includes: the user A and B for attempting to agree to key, issues negotiation signal from A to B, B generates secret at random in real time Close several N_BAfterwards to N_BIt carries out Hash operation and obtains hash (N_B), and send A to； A generates X and carries out encryption meter using converter Calculate V=enc (hash (mk, hash (N_B)),hash(X))； A sends V value to B, and B is by V value and N_BValue is input to converter, Converter, which is decrypted, calculates dec (hash (mk, hash (N_B)), V), calculated result should be equal to hash (X), A and B by Hash (hash (X)) is agreed on public credit channel finally to confirm keyed hash hash (X), wherein mk is all converters The master key all known, other people can not know that the master key, enc and dec are the encryption that symmetric key is used in converter And decryption function.

17. according to claim 16 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: all communications including the final confirmation can be completed on Dolev-Yao network.

18. according to claim 12 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: compound function needed for the converter has the function of calculating A and B.

19. according to claim 16 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: B by hash (N_B) it is re-used as disposable or nonexpondable public key, if B is in same type exchange by hash (N_B) conduct One or many public keys used, without making change to function, so that it may obtain privacy key N_B。

20. according to claim 12 for the public key encryption of block chain and the creation equipment of key signature, feature exist In: for the X that signs, inputs X and private key sk and export enc (hash (ms, hash (sk)), X)； It is verified by public key pk, The step of verifying includes: input Y and pk, is exported dec (hash (ms, pk), Y).Verifying agency checks the lattice of the signature X Whether formula is correct and/or the signature X is equal to the signature X known otherwise； Ms is that another all converter is all known The key of dawn, other people can not know the master key, and it is to use in converter that ms, which must be different from master key mk, enc and dec, In the encryption and decryption function of symmetric key.

21. according to claim 20 for the public key encryption of block chain and the creation equipment of key signature, feature exist It is also used to crack encryption in the step of: verifying.

22. 6 or 20 is any described for the public key encryption of block chain and the creation equipment of key signature according to claim 1, It is characterized by: being removed using the function f for being easy to calculate so that dec (k) and enc (f (k)) are identical for symmetric cryptography Non- f be immobilize or comprising a large amount of k in the case where, otherwise can eliminate the angle-of-attack using Hash operation.

23. a kind of machine readable storage medium, is stored thereon with computer program, wherein the computer program is by processor When execution realize as described in claim 12-22 is any for the public key encryption of block chain and the creation method of key signature.

Description

The creation method of public key encryption and key signature, equipment and readable storage medium storing program for executing

Technical field

The present invention relates to the creation method of block chain technical field more particularly to a kind of public key encryption and key signature, set Standby and readable storage medium storing program for executing.

Background technique

Shor algorithm is extremely important, it is represented using in the case where quantum computer, can be made extensively for cracking Public key encryption method, i.e. RSA cryptographic algorithms, the basis of RSA Algorithm are the assumption that we cannot very effectively decompose One known integer, Shor algorithm illustrate Factorization this problem available effectively solution on quantum computer Certainly, so that a sufficiently large quantum computer can crack RSA.Currently, Shor algorithm greatly advances quantum meter The development of calculation machine also promotes the realization for physically realizing quantum computer.The algorithm does not ensure that each operation can It obtains correctly as a result, still a kind of random algorithm can be belonged to by the probability of the number increase Success in Experiment of increase experiment.

The safety of common key cryptosystem depends primarily on the mathematical problem that construction algorithm is relied on, it requires encryption function With one-way, that is, the difficulty inverted, thus cryptanalysis person will obtain privacy key for current from public-key cryptography It is infeasible for computing capability.

Public key cryptography is the method for an encryption data under the public key of agency, and result can only use almost impossible The corresponding privacy key that obtains is calculated from public key to decrypt.Conventionally this is calculated by cleverly mathematical function for we , these mathematical functions meet this specification naturally, however quantum calculation changes unpredictably, we do not know for sure actually letter Achieved by number what is on earth, this point needs to pay attention to.With the arrival in quantum calculation epoch, the world keeps inherently safe Mode have become an important problem, numerous studies concentrate on not vulnerable to the signature of quantum computer attack and non-right Claim cryptographic system.However, these can not directly be solved the problems, such as, because these obviously cannot provide specific alternative scheme. In addition, most of work is dedicated to the cryptography based on grid, this is considered as most promising asymmetric cryptography solution, However it is not using fundamental cryptographic, rather increases scheme complexity.

It is generally believed that the cryptographic Hash method of standard be or can accomplish it is not pregnable, and have it is sufficiently strong Symmetric cryptosystem, such as AES.Reasonable scheme be more willing to follow on fundamental cryptographic basis increase it is simple with can be real Existing technique complementary.

Summary of the invention

In view of above-mentioned technical problem, the present disclosure presents a kind of public key encryption and key signature creation methods, equipment And readable storage medium storing program for executing, it only uses symmetric cryptography and hash function safely exchanges key, thus with basic and very effective The password that mode creates authenticity, integrality and non-repudiation proves, creation is allowed encrypt and by secret using public key The equipment of key decryption, or creation and verifying, using the equipment of the signature of key creation, these simply encrypt equipment not It can be by successfully reverse-engineering.

Inventive conception is that: solution provided by the present invention avoid used in ciphering process asymmetric plus The risk that decryption method is cracked by quantum computer uses a converter, there is computations program enc, decryption in converter Calculation procedure dec, secret value mk and other required necessary programs, it is in need transmitting information converter in have this secret Close value mk, is consistent, and the value is not to avoid key in symmetric encryption method in this way known to other sides and pass Defeated safety problem.This converter can be applied not only to the encryption of block chain, can be also used for other encryption applications. To use public key encryption mode, the present invention also provides a kind of methods, are extended to above-mentioned converter function, increase another The only converter secret value ms that knows and be consistent in different switching device proposes the computations program enc reconciliation of extension Close calculation procedure dec realizes verifying and other associated encryption applications to public key.

In the one aspect of present disclosure, a kind of creation of public key encryption and key signature for block chain is provided Method, comprising:

Step S101, constructor, to meet the encryption data under public key, the side for possessing converter creates message, It is only used the corresponding addressee of public key that could decrypt, can only be come using the corresponding privacy key obtained cannot be calculated from public key Decryption, to realize the public key encryption creation of block chain；

Step S102 selects to create different secret values from the public key encryption of block chain is realized, shared for all converters, Its other party can not know, by Hash operation and verification step, verifying agency check signature format whether correctly and/or whether Signature is equal to another signature known otherwise.

In some embodiments, the function is supplied to user as integrated package, and refusal attacker, which gets around, to be divided The chance of the function is solved, and a part of the public key is retained into the secret value in the integrated package, thus institute Stating public key can not be from reconstruction.

In some embodiments, a variety of secure key negotiation methods, the secure key negotiation are carried out using converter Method using self-generating entropy method or by user's formation entropy method, the method by user's formation entropy include to entropy into Row Hash operation prevents the attack of third side.

In some embodiments, it is generated for the agreement finally developed, self-generating entropy method and by user The method of entropy includes: to carry out Hash operation to entropy to prevent the attack of third side.

In some embodiments, the step S101 includes: the user A and B for attempting to agree to key, they are respectively Possess converter, issue negotiation signal from A to B when transmitting starts, B generates secret number N at random in real time$_B$Afterwards to N$_B$Carry out Hash fortune Calculation obtains hash (N$_B$), and send A to； A generates X and carries out computations V=enc (hash (mk, hash using converter (N$_B$)),hash(X))； A sends V value to B, and B is by V value and N$_B$Value is input to converter, and converter, which is decrypted, calculates dec (hash(mk,hash(N$_B$)), V), calculated result should be equal to hash (X), A and B by agreeing on public credit channel Hash (hash (X)) is finally to confirm keyed hash hash (X), and wherein mk is the master key that all converters all know, Other people can not know that the master key, enc and dec are the encryption and decryption function that symmetric key is used in converter.

In some embodiments, all communications including the final confirmation can be in Dolev-Yao network Upper completion.

In some embodiments, the converter has the function of compound function needed for calculating A and B.

In some embodiments, B is by hash (N$_B$) it is re-used as disposable or nonexpondable public key, if B is same By hash (N in type exchange$_B$) as one or many public keys used, without making change to function, so that it may obtain secret Key N$_B$。

In some embodiments, the step S102 includes: and inputs X and private key sk for the X that signs and export enc (hash(ms,hash(sk)),X)； It is verified by public key pk, the step of verifying includes: input Y and public key pk, defeated Dec (hash (ms, pk), Y) out.Verifying agency checks whether the format of the signature X correct and/or the signature X is equal to and leads to Cross the signature X that other way is known； Ms is the key that another all converter all knows, other people can not know that the master is close Key, and it is the encryption and decryption function that symmetric key is used in converter that ms, which must be different from master key mk, enc and dec,.

In some embodiments, the step of verifying is also used to crack encryption.

In some embodiments, for symmetric cryptography using the function f for being easy to calculate, so that dec (k) and enc (f (k)) identical, unless f be immobilize or comprising a large amount of k in the case where, otherwise can eliminate this using Hash operation and attack Hit angle.

In the another aspect of present disclosure, the wound of a kind of public key encryption for block chain and key signature is additionally provided Standby, including processor is built, wherein the processor can be used for:

Constructor, to meet the encryption data under public key, the side for possessing converter creates message, is only used The corresponding addressee of public key could decrypt, and can only be decrypted using that cannot calculate the corresponding privacy key obtained from public key, thus Realize the public key encryption creation of block chain；

Selection with realize block chain public key encryption create different secret values, for all converters share, other party without Method knows, by Hash operation and verification step, whether verifying agency, which checks whether signature format is correct and/or sign, is equal to Another signature known otherwise.

In some embodiments, the function is supplied to user as integrated package, and refusal attacker, which gets around, to be divided The chance of the function is solved, and a part of the public key is retained into the secret value in the integrated package, thus institute Stating public key can not be from reconstruction.

In some embodiments, a variety of secure key negotiation methods, the secure key negotiation are carried out using converter Method using self-generating entropy method or by user's formation entropy method, the method by user's formation entropy include to entropy into Row Hash operation prevents the attack of third side.

In some embodiments, it is generated for the agreement finally developed, self-generating entropy method and by user The method of entropy includes: to carry out Hash operation to entropy to prevent the attack of third side.

In some embodiments, the function includes: the user A and B for attempting to agree to key, issues and assists from A to B Quotient's signal, B generate secret number N at random in real time$_B$Afterwards to N_BIt carries out Hash operation and obtains hash (N_B), and send A to； A generates X simultaneously And computations V=enc (hash (mk, hash (N is carried out using converter$_B$)),hash(X))； A sends V value to B, and B is by V Value and N_BValue is input to converter, and converter, which is decrypted, calculates dec (hash (mk, hash (N_B)), V), calculated result should Equal to hash (X), A and B on public credit channel by agreeing to hash (hash (X)) finally to confirm keyed hash hash (X), wherein mk is master key that all converters all know, other people can not know that the master key, enc and dec are conversion The encryption and decryption function of symmetric key are used in device.

In some embodiments, all communications including the final confirmation exist

It is completed on Dolev-Yao network.

In some embodiments, the converter has the function of compound function needed for calculating A and B.

In some embodiments, B is by hash (N_B) it is re-used as disposable or nonexpondable public key, if B is same By hash (N in type exchange$_B$) as one or many public keys used, without making change to function, so that it may obtain secret Key N_B。

In some embodiments, for the X that signs, input X and private key sk and export enc (hash (ms, hash (sk)), X)； It is verified by public key pk, the step of verifying includes: input Y and pk, is exported dec (hash (ms, pk), Y).It tests Card agency checks whether the format of the signature X is correct and/or the signature X is equal to the signature X known otherwise； ms For the key that another all converter all knows, other people can not know the master key, and ms must be different from master key Mk, enc and dec are the encryption and decryption function that symmetric key is used in converter.

In some embodiments, the step of verifying is also used to crack encryption.

In some embodiments, for symmetric cryptography using the function f for being easy to calculate, so that dec (k) and enc (f (k)) identical, unless f be immobilize or comprising a large amount of k in the case where, otherwise can eliminate this using Hash operation and attack Hit angle.

In present disclosure in another aspect, additionally provide a kind of machine readable storage medium, it is stored thereon with computer Program, wherein the computer program realize when executed by the processor the public key encryption for block chain as described above and The creation method of key signature.

Compared with prior art, present disclosure has the beneficial effect that

The exchange key of symmetric cryptography and hash function safety is only used, to create in a manner of basic and is very effective The password of authenticity, integrality and non-repudiation proves, creation is allowed encrypt and by privacy key solution using public key Close equipment, or creation and verifying, using the equipment of the signature of key creation, these simply encrypt equipment cannot be by success Ground reverse-engineering.

Detailed description of the invention

It has been specifically explained in the appended claims novel feature of the invention.By reference to using this wherein The features as discussed above that the illustrated embodiment of inventive principle is illustrated, it will to the features and advantages of the present invention It is better understood from.Attached drawing is only used for showing the purpose of embodiment, and should not be considered limitation of the present invention.And And throughout the drawings, identical element is presented with like reference characters, in the accompanying drawings:

Fig. 1 shows the public key encryption and key signature for block chain according to present disclosure illustrative embodiments Creation method flow chart； And

Fig. 2 shows the public key encryptions and key signature for block chain according to present disclosure illustrative embodiments Creation device structure schematic diagram.

Specific embodiment

The illustrative embodiments of present disclosure are more fully described below with reference to accompanying drawings.Although being shown in attached drawing The illustrative embodiments of present disclosure, it being understood, however, that may be realized in various forms present disclosure without should be by Embodiments set forth herein is limited.It is to be able to thoroughly understand in the disclosure on the contrary, providing these embodiments Hold, and can will scope of the present disclosure be completely communicated to those skilled in the art.Do not have in the following detailed description Any content is intended to indicate that any specific components, feature or step are essential for the present invention.Those skilled in the art It will be understood that scope of the present disclosure interior various features or step to substitute or combine each other not departing from.

Solution provided by the present embodiment avoids the asymmet-ric encryption method used in ciphering process by quantum meter The risk that calculation machine cracks uses a converter in implementation, there is computations program enc, decryption calculation procedure in converter Dec, secret value mk and other required necessary programs, it is in need transmitting information converter in have secret value mk, It is consistent, and the value is not to avoid the peace of cipher key delivery in symmetric encryption method in this way known to other sides Full problem.This converter can be applied not only to the encryption of block chain, can be also used for other encryption applications.To use Public key encryption mode, the present invention also provides a kind of methods, are extended to above-mentioned converter function, increase another and only turn The secret value ms that parallel operation is known and is consistent in different switching device proposes that the computations program enc of extension and decryption are calculated Program dec realizes verifying and other associated encryption applications to public key.

Fig. 1 shows the public key encryption and key signature for block chain according to present disclosure illustrative embodiments The flow chart of creation method.As shown in Figure 1, a kind of for the public key encryption of block chain and the creation method of key signature, packet It includes:

Step S101, constructor, to meet the encryption data under public key, the side for possessing converter creates message, It is only used the corresponding addressee of public key that could decrypt, can only be come using the corresponding privacy key obtained cannot be calculated from public key Decryption, to realize the public key encryption creation of block chain；

Step S102 selects to create different secret values from the public key encryption of block chain is realized, shared for all converters, Its other party can not know, by Hash operation and verification step, verifying agency check signature format whether correctly and/or whether Signature is equal to another signature known otherwise.

In this embodiment, if we just can have an opportunity function decomposition, attacker to get around these functions, Therefore the function is supplied to user as integrated package, and refusal attacker gets around the chance for decomposing the function, and A part of the public key is retained into the secret value in the integrated package, so that the public key can not be from reconstruction.

In this embodiment, a variety of secure key negotiation methods, the secure key negotiation side are carried out using converter For method using self-generating entropy method or by the method for user's formation entropy, the method by user's formation entropy includes carrying out to entropy Hash operation prevents the attack of third side.

In this embodiment, for the agreement finally developed, self-generating entropy method and by user's formation entropy Method include: to carry out Hash operation to entropy to prevent the attack of third side.

In this embodiment, the step S101 includes: the user A and B for attempting to agree to key, they respectively gather around There is converter, issue negotiation signal from A to B when transmitting starts, B generates secret number N at random in real time$_B$Afterwards to N_BCarry out Hash operation Obtain hash (N_B), and send A to； A generates X and carries out computations V=enc (hash (mk, hash using converter (N_B)),hash(X))； A sends V value to B, and B is by V value and N_BValue is input to converter, and converter, which is decrypted, calculates dec (hash(mk,hash(N_B)), V), calculated result should be equal to hash (X), A and B by agreeing on public credit channel Hash (hash (X)) is finally to confirm keyed hash hash (X), and wherein mk is the master key that all converters all know, Other people can not know that the master key, enc and dec are the encryption and decryption function that symmetric key is used in converter.

It in this embodiment, can be on Dolev-Yao network including all communications within the final confirmation It completes.

In this embodiment, the converter has the function of compound function needed for calculating A and B.

In this embodiment, B is by hash (N_B) it is re-used as disposable or nonexpondable public key, if B is similar By hash (N in type exchange$_B$) as one or many public keys used, without making change to function, so that it may obtain secret Key N_B。

In this embodiment, the step S102 includes: and inputs X and private key sk for the X that signs and export enc (hash (ms,hash(sk)),X)； It is verified by public key pk, the step of verifying includes: input Y and pk, exports dec (hash (ms,pk),Y).Verifying agency checks whether the format of the signature X is correct and/or the signature X is equal to otherwise The signature X known； Ms is the key that another all converter all knows, other people can not know the master key, and ms must It is the encryption and decryption function that symmetric key is used in converter that master key mk, enc and dec, which must be different from,.

In this embodiment, the step of verifying is also used to crack encryption.

In this embodiment, for symmetric cryptography using the function f for being easy to calculate, so that dec (k) and enc (f (k)) identical, unless f be immobilize or comprising a large amount of k in the case where, otherwise can eliminate this using Hash operation and attack Hit angle.

Assuming that there are a general addressable time stamp data library, as the public key encryption equipment of block chain, building has It is such as properties:

First, identical equipment or the equipment of a small amount of type by role's characterization are widely distributed, and by it is all by Letter side and potential attacker co-own, and equipment can be interacted safely with its owner, and pass through uneasiness under some cases Full network is interactively with each other；

Second, multiple numerical value are calculated or communicated according to publicly available art methods in equipment, but are only permitted to hold Have and secret value be all disabled to external multi-party and equipment own user, the secret value in all examples on an equal basis creation or Person is created in calculating process；

Third, equipment without using public key or other there are the encryption technology of potential quantum loophole, the affected meters of equipment A small amount of and economy is higher at last；

4th, equipment makes its user exchange or develop the key that other each side can not all know；

In the present embodiment, setting Alice and Bob is attempt to two users of confirmation key, possesses converter A and B respectively, Keyed hash hash (X) can be generated by following agreement, Alice and Bob can be by confirming hash on public credit channel (hash(X)).It can be completed on Dolev-Yao network including all communications within the final confirmation.

Mk is the master key that all converters all know, other people can not know the master key.So agreement process It can be characterized using following code:

Alice- > Bob: start；

Bob generates N at random in real time$_B$；

Bob- > Alice: to N_BIt carries out Hash operation and obtains hash (N_B)；

Alice generates X and carries out computations V=enc (hash (mk, hash (N using A_B)),hash(X))；

Alice- > Bob: V is sent；

Bob is by V value and N_BValue is given to B, and B, which is decrypted, calculates dec (hash (mk, hash (N_B)), V), result is answered When equal to hash (X).

Here enc and dec is the operation carried out in converter, can use the encryption and decryption of some suitable symmetric keys Function.Converter must have there are two function, i.e. encrypting and decrypting compound function needed for calculating Alice and calculate needed for Bob Encrypting and decrypting compound function.

In the present embodiment, N_BFor a secret value, only Bob knows and is used to be calculated last keyed hash hash (X), the corresponding calculating function of value transmitted by Alice and Bob converter is needed when calculating.

If Bob reuses N in following same type exchange$_B$, then too many change is not had, but Bob is also It has no longer at the beginning of agreement with Hash hash (N_B) form send disposable N_BHave between final received message direct Causality.Under any circumstance, Bob guarantee to be administered is all seldom, because anyone can send out to it in any case Send the Hash hash (N with overhead$_B$) final message.Agreement determined by the present embodiment ensure in addition to use A and The Hash hash (X) at agreement end can be known using nobody except the user of B, and is known in view of the identity for lacking converter Other information, just can not more know more information.Alice and Bob can only be compared by the Hash hash (X) in public credit channel Compared with identification other side, therefore, Bob is possible to Hash hash (N_B) it is re-used as disposable or nonexpondable public key.Know this Anyone of a cryptographic Hash successfully can send the message in above-mentioned agreement to Bob, since Bob knows N_BContent, Converter can be decoded accurately, therefore N_BIt is public key Hash hash (N_B) privacy key.This is an ideal pairing, because Difficulty to derive key by public key is exactly the preimage resistance of cryptographic Hash function.

The above agreement is not proper public key encryption, because X is used for the input of " encryption ", hash (X) is by " solution It is close ", and it is to prevent the decryption of third side from destroying the reason of Hash calculation.Without Hash operation, Alice can be not intended to X is sent to Eve by the case where knowledge, and then X can be sent to Bob by Eve, and Alice and Bob can not perceive this point. In addition, if Alice knows Hash Hash (N_B) it is by Bob rather than Eve is generated, then above situation becomes impossible , because Eve needs to create the Hash Hash (N of oneself in such MITM attack$_B$), so as to use turning for itself The decryption function of parallel operation, in such a case, it is possible to remove the Hash operation of " X " from " encryption ", then Alice can know Dawn only has Bob that can decrypt its information.

It is pk that each node, which has registered with a form,$_A$=hash (sk_A) the public key by Certificate Authority, these are recognized Card authorization endorsed key certificate appropriate for it.Given X and pk, converter will calculate for the user under encryption mode enc(hash(mk,pk),X).For give Y and sk, converter calculate decryption mode under dec (hash (mk, hash (sk)), Y), the effect of exactly desired public key encryption.Any people for possessing converter can create a piece of news, only use public key Addressee could decrypt.The converter information receiving and transmitting function that realizes asymmetric encryption in this way.

Decryption is difficult to manipulate the conversion on key, because the almost impossible reversion of process, and reach illegal by building Purpose is decrypted, as the specification of public key encryption is decomposed into multiple component parts by us.Certainly, the public affairs of this structure design Disadvantage that there are two key cryptography tools, first, original evidence is not provided； Second, as long as can guess out in plain text, it can be examined It looks into, however, this is can to overcome first disadvantage by signature, and prevent second disadvantage by spreading, i.e., in encryption It is preceding to be randomly chosen multiple enough as filling.

Cryptologist mostly uses public key encryption algorithm to sign, if Alice encrypts certain things with its key, Anyone can be decrypted by using the public key of Alice to verify, however the operation implements common recognition mechanism due to not having Function and become nonsensical.It is not suitable for decrypting sk, then the encryption at pk executes this operation, unless bottom symmetric adds yet The close encryption having after being decrypted using the same key is the attribute of identity function.Turn however, the embodiment can extend The creation that parallel operation function is signed: it for the X that signs, inputs X and sk and exports enc (hash (ms, hash (sk)), X)； Pass through The step of pk is verified includes: input Y and pk, is exported dec (hash (ms, pk), Y).Verifying agency can check that format is It is no correct and/or be the key that another all converter all knows equal to some X known otherwise, ms, other People can not know the master key, and it is in converter for symmetric key that ms, which must be different from master key mk, enc and dec, Encryption and decryption function.If secret value ms is equal with mk, which will be easy to be cracked.

The problem of agreement above is able to solve public key encryption, for whether needing to avoid the demand of reverse-engineering not relate to And.Under this hypothesis, see under encryption mode it is dangerous it is main it is potential for given encryption enc (hash (mk,)), pk there is the converter with multiple features provided by a kind of use still can be to it in the case where not knowing sk The method of decryption.If enc (k, enc (k, x))=x or acquisition can therefrom derive the element of X, then the agreement just becomes It obtains without value, therefore needs are careful when selection symmetric cryptography, otherwise assumes to tie using Hash in key structure and result The almost impossible any specific purpose for reaching encryption key of fruit.For certain symmetric cryptographies, using the function f for being easy to calculate, So that dec (k) and enc (f (k)) it is identical, unless f be immobilize or comprising a large amount of k in the case where, otherwise use Hash operation eliminates the angle-of-attack of the encryption method.This is for some other key structure and is not suitable for.Same makes With Hash operation, and use different mk and ms numerical value, it is not necessary to worry mutually dry between the encryption of converter and signature scheme It disturbs, even if the character string that attacker freely inputs any correct length under either mode is exported instead of the Hash of pk, also not It must interference between worry mode.And for any specific symmetric encryption method, consider that its working method in framework is related Autonomous behavior, however equally will not switching between Effect Mode.

Fig. 2 shows a kind of public key encryptions and key for block chain according to present disclosure illustrative embodiments The structural schematic diagram of the creation equipment of signature.As shown in Fig. 2, the creation of the public key encryption and key signature that are used for block chain is set Standby includes processor 201, and wherein processor 201 can be used for the public key encryption of block chain and the creation method of key signature, Include:

Step S101, constructor, to meet the encryption data under public key, the side for possessing converter creates message, It is only used the corresponding addressee of public key that could decrypt, can only be come using the corresponding privacy key obtained cannot be calculated from public key Decryption, to realize the public key

encryption creation of block chain；

Step S102 selects to create different secret values from the public key encryption of block chain is realized, shared for all converters, Its other party can not know, by Hash operation and verification step, verifying agency check signature format whether correctly and/or whether Signature is equal to another signature known otherwise.

In this embodiment, if we just can have an opportunity function decomposition, attacker to get around these functions, Therefore the function is supplied to user as integrated package, and refusal attacker gets around the chance for decomposing the function, and A part of the public key is retained into the secret value in the integrated package, so that the public key can not be from reconstruction.

In this embodiment, a variety of secure key negotiation methods, the secure key negotiation side are carried out using converter For method using self-generating entropy method or by the method for user's formation entropy, the method by user's formation entropy includes carrying out to entropy Hash operation prevents the attack of third side.

In this embodiment, for the agreement finally developed, self-generating entropy method and by user's formation entropy Method include: to carry out Hash operation to entropy to prevent the attack of third side.

In this embodiment, the step S101 includes: the user A and B for attempting to agree to key, is issued from A to B Negotiation signal, B generate secret number N at random in real time$_B$Afterwards to N_BIt carries out Hash operation and obtains hash (N_B), and send A to； A generates X And computations V=enc (hash (mk, hash (N is carried out using converter$_B$)),hash(X))； A sends V value to B, and B will V value and N_BValue is input to converter, and converter, which is decrypted, calculates dec (hash (mk, hash (N_B)), V), calculated result is answered When be equal to hash (X), A and B by public credit channel agree to hash (hash (X)) finally to confirm the keyed hash Hash (X), wherein mk is the master key that all converters all know, other people can not know that the master key, enc and dec are The encryption and decryption function of symmetric key are used in converter.

In this embodiment, all communications including the final confirmation can be

It is completed on Dolev-Yao network.

In this embodiment, the converter has the function of compound function needed for calculating A and B.

In this embodiment, B is by hash (N_B) it is re-used as disposable or nonexpondable public key, if B is similar By hash (N in type exchange$_B$) as one or many public keys used, without making change to function, so that it may obtain secret Key N_B。

In this embodiment, the step S102 includes: to have registered in all nodes by Certificate Authority When public key sk, converter can carry out public key encryption and verifying.For the X that signs, inputs X and private key sk and export enc (hash (ms,hash(sk)),X)； It is verified by public key pk, the step of verifying includes: input Y and public key pk, exports dec (hash (ms, pk), Y), verifying agency checks whether the format of the signature X correct and/or the signature X be equal to pass through it is other The signature X that mode is known； Ms is the key that another all converter all knows, other people can not know the master key, and It is the encryption and decryption function that symmetric key is used in converter that ms, which must be different from master key mk, enc and dec,.

In this embodiment, the step of verifying is also used to crack encryption.

In this embodiment, for symmetric cryptography using the function f for being easy to calculate, so that dec (k) and enc (f (k)) identical, unless f be immobilize or comprising a large amount of k in the case where, otherwise using Hash operation, can to eliminate this right Claim the angle-of-attack of Encryption Algorithm.

In present disclosure in another aspect, additionally provide a kind of machine readable storage medium, it is stored thereon with computer Program, wherein the computer program realize when executed by the processor the public key encryption for block chain as described above and The creation method of key signature.It is above for the technical solution of the creation of public key encryption and key signature for block chain Detailed description has been carried out, details are not described herein.In some embodiments, machine readable storage medium is that digital processing is set Standby tangible components.In other embodiments, machine readable storage medium is optionally that can remove from digital processing device 's.In some embodiments, lift non-limiting example for, machine readable storage medium may include USB flash disk, mobile hard disk, Read-only memory (ROM, Read-Only Memory), is dodged random access memory (RAM, Random Access Memory) Fast memory, programmable read only memory (PROM), Erasable Programmable Read Only Memory EPROM (EPROM), solid-state memory, magnetic Dish, CD, cloud computing system or service etc..

It should be appreciated that each step recorded in the method implementation of present disclosure can be held in a different order Row, and/or parallel execution.In addition, method implementation may include additional step and/or omit the step of execution is shown. The scope of the present invention is not limited in this respect.

In descriptions provided herein, numerous specific details are set forth.It will be appreciated, however, that present disclosure Embodiment can be practiced without these specific details.In some embodiments, it is not been shown in detail known Methods, structures and technologies, so as not to obscure the understanding of this specification.

It is aobvious for those skilled in the art although exemplary embodiments of the present invention have been illustrated and described herein And be clear to, such embodiment only provides in an illustrative manner.Those skilled in the art now will without departing from Many changes are expected in the case where the present invention, are changed and are substituted.It should be appreciated that practice the present invention during can using pair The various alternative solutions of embodiments of the invention described herein.Following following claims is intended to limit the scope of the invention, and Therefore the method and structure and its equivalent item in these scopes of the claims are covered.

Similar Documents

Publication	Publication Date	Title
CN101529791B	2017-06-06	Using a low complexity means for providing privacy and authentication methods and apparatus
US6535980B1	2003-03-18	Keyless encryption of messages using challenge response

US8059818B2	2011-11-15	Accessing protected data on network storage from multiple devices
Piper	2002	Cryptography
JP4527358B2	2010-08-18	Do not use a key escrow, authenticated individual cryptographic system
US20100174911A1	2010-07-08	Anonymous authentication system and anonymous authentication method
Lee et al.	2012	An extended chaotic maps-based key agreement protocol with user anonymity
Ali et al.	2017	SeDaSC: secure data sharing in clouds
JP4944886B2	2012-06-06	Technique with a safety improved relative malleability attacks using a signature key encrypted with a non-OTP cipher including (but not limited to), encrypted authentication, and / or sets of shared secret
Tseng et al.	2009	A chaotic maps-based key agreement protocol that preserves user anonymity
WO2016065321A1	2016-04-28	Secure communication channel with token renewal mechanism
CN1186580A	1998-07-01	Computer-assisted method for exchange of crytographic keys between user computer and network computer unit
US5539826A	1996-07-23	Method for message authentication from non-malleable crypto systems
US20120023336A1	2012-01-26	System and method for designing secure client-server communication protocols based on certificateless public key infrastructure
US7634085B1	2009-12-15	Identity-based-encryption system with partial attribute matching
JP2012050066A	2012-03-08	Secure field-programmable gate array (fpga) architecture
JP2000124887A	2000-04-28	Enciphering/decoding method for group unit, and method and device for signature
US8688973B2	2014-04-01	Securing communications sent by a first user to a second user
US6640303B1	2003-10-28	System and method for encryption using transparent keys
Zhang et al.	2014	Efficient and flexible password authenticated key agreement for voice over internet protocol session initiation protocol using smart card
CA2521549A1	2006-04-19	Cryptographic communications session security
CN103338448A	2013-10-02	Wireless local area network security communication method based on quantum key distribution
CN102624522A	2012-08-01	Key encryption method based on file attribution
CN101032117A	2007-09-05	Method of authentication based on polynomials
KR100582546B1	2006-05-22	Method for sending and receiving using encryption/decryption key

Priority And Related Applications

Priority Applications (1)

Application	Priority date	Filing date	Title
CN201811300417.4A	2018-11-02	2018-11-02	The creation method of public key encryption and key signature, equipment and readable storage medium storing program for executing

Applications Claiming Priority (1)

Application	Filing date	Title
CN201811300417.4A	2018-11-02	The creation method of public key encryption and key signature, equipment and readable storage medium storing program for executing

Legal Events

Date	Code	Title	Description
2019-01-25	PB01		
2019-02-26	SE01		