Open Access Library Journal
2022, Volume 9, e8287
ISSN Online: 2333-9721
ISSN Print: 2333-9705

CPK Public Key and Its Basic Functions

Xianghao Nan

CPK Laboratory, Beijing, China
Email: nanxianghao@bochtec.com

How to cite this paper: Nan, X.H. (2022) CPK Public Key and Its Basic Functions. *Open Access Library Journal*, **9**: e8287.
https://doi.org/10.4236/oalib.1108287

Received: December 10, 2021
Accepted: January 11, 2022
Published: January 14, 2022

Abstract

This paper introduces the working principle of CPK (Combined Public Key) and the general method of constructing identifier-based public key, which can not only solve the problem of key distribution, but also solve the authentication problem of identifier claimed by the subject. As basic functions, identifier authentication, identifier password, digital signature and key encryption are introduced. Where Identifier authentication is a new concept, and a separate authentication protocol is formulated to prove the authenticity of identifier. Identifier password is an asymmetric password, constructed with identifier authentication technique which can not only identify the authenticity of password, but also prove the authenticity of the subject, and prevent illegal access and DOS attacks. Digital signature is based on identifier authentication, which makes DSS become the digital signature standard in real sense. The key encryption implements encrypted communication between any two points on the open public network, reducing the closing segmentation granularity to the sender and receiver, making the extra regional segmentation redundant.

Subject Areas

Information and Communication, Security, Privacy, and Trust

Keywords

Authentication, Digital Signature, Password, Encryption

1. Introduction

In modern public key system, public-key distribution has been a difficult problem. In 1984, Shamir first proposed the concept that identifier can directly be taken as a public-key [1], and constructed an identifier-based public key scheme IBS with factor decomposition. Even though it didn't work out, it pointed out the direction for the development of public key system. CPK (Combined Public

Key) [2] is a general approach to transform existing public key schemes into identifier-based public key schemes.

Now CPK has formed into a large family, including CPK-$_{RSA}$ based on factor decomposition problem, CPK-$_{DLP}$ based on discrete logarithm problem, CPK-$_{ECC}$ based on elliptic curve problem, CPK-$_{CCC}$ based on conic curve [3], CPK-$_{BLP}$ based on bilinear pairing, etc., where the signature code of CPK-$_{ECC}$ is the shortest.

Later, it is found that the identifier-based public key can not only solve the problem of public-key distribution, but also solve the problem of subject authenticity proof, which has been the core technology of cyber security.

The following takes CPK-$_{ECC}$ as an example to introduce the original type and smart type of CPK.

2. CPK Original Type

2.1. Combining Principle

CPK-$_{ECC}$ is constructed on ECC [4] [5] over field Fp, $\mathrm{E}: y^2 = \left(x^3 + ax + b\right) \bmod p$, the parameters are denoted as (a, b, G, n, p), in which a, b is coefficient, $a, b, x, y \in \mathrm{F}p$, p is prime, G is the base point of the addition group, n is the order of group generated by base point G. Let an arbitrary integer $r \in \mathrm{F}n$ be a private-key, then the point, $rG = R$, is the corresponding public-key. The ECC has a compounding feature: the sum of public-keys and the sum of corresponding private-keys are still the valid key pairs. For example, if the sum of private-keys is:

$$r = \left(r_1 + r_2 + \cdots + r_m\right) \bmod n$$

and the sum of corresponding public-keys will be

$$R = R_1 + R_2 + \cdots + R_m$$

then (r, R) will be a new key pair. This is because

$$\begin{aligned} R &= R_1 + R_2 + \cdots + R_m = r_1 G + r_2 G + \cdots + r_m G \\ &= \left(r_1 + r_2 + \cdots + r_m\right) G = rG \end{aligned}$$

In the same way, if a given integer is less than n, the following formula is established:

r and R are a pair of keys, if k times of r is the new private-key s, then the k times of R is the corresponding public-key:

$$k * r = s; \quad k * R = S$$

If the private-key r plus k is t, then R plus K is the new public-key T:

$$r + k = t; \quad R + K = T \quad \left(K = k * G\right)$$

2.2. Combination Matrix

Combining-Matrix is divided into private matrix and public matrix, and is denoted as ($r_{i,j}$) and ($R_{i,j}$) respectively, where r is hx32 random integers less than n, and not all linear independent. Matrix ($r_{i,j}$) is kept secret only in key manage-

ment ceter(KMC), and is used to produce private-keys for individual entity. The public matrix ($R_{i,j}$) is derived from private matrix ($r_{i,j}$), the relation is $r_{i,j} \cdot G = R_{i,j}$.

Private Matrix(a) Public Matrix(A)

$$a = \begin{pmatrix} r_{0,0} & r_{0,1} & \cdots & r_{0,31} \\ r_{1,0} & r_{1,1} & \cdots & r_{1,31} \\ \vdots & \vdots & \ddots & \vdots \\ r_{h,0} & r_{h,1} & \cdots & r_{h,31} \end{pmatrix} \quad A = \begin{pmatrix} R_{0,0} & R_{0,1} & \cdots & R_{0,31} \\ R_{1,0} & R_{1,1} & \cdots & R_{1,31} \\ \vdots & \vdots & \ddots & \vdots \\ R_{h,0} & R_{h,1} & \cdots & R_{h,31} \end{pmatrix}$$

Public matrix is distributed to every entity and used to compute the public-key of relying party.

2.3. Key Combination

The key management center defines the Hash key Hkey. The given identifier is hashed to YS sequence under Hkey, to take the matrix size 32 × 32 as example:

$$\mathrm{YS} = \mathrm{Hash}_{\mathrm{Hkey}i}\left(\mathrm{Identifier}\right) = v_0, v_1, v_2, \cdots, v_{31};$$

Row coordinates of the matrix are indicated by v_i, and column ordinates are used in natural order. Alice's key pair are combined as

$$\mathrm{Alice}_{sk} = \sum_{i=0}^{31} r_{[v_i,i]} \bmod n = alice$$

$$\mathrm{Alice}_{PK} = \sum_{i=0}^{31} R_{[v_i,i]} = ALICE$$

2.4. Open Problem

In 2003, the release of CPK aroused strong response and high attention at home and abroad, and set off an upsurge across the country. Since the private-key is a linear combination of matrix variables, linear equations can be listed. Since it was not so assrued, the matrix size is given $h \times 32$ (h = 32..1024). By algebraic theorem, linear equations have solutions, and when linear dependent equations have infinite solutions, it is nothing to do with collusion, but linear independent equations with full rank, have unique solutions, whereas linear independent equations are not easy to construct, while linear dependent equations are easy to construct. It had been an open problem. In 2006, the competent authority suddenly came to the opposite conclusion: "Linear correlation of equations leads to collusion," and launched a nationwide crackdown in an attempt to kill it with one stick.

Despite the harsh environment, the research work did not stop. In the study, it was also found that CPK has countless equivalent matrices, but it was not clear whether harmful. In order to change the static matrix into the dynamic matrix, a hierarchy parameter *fcc* and annual key *year* were set in the improved CPK [6]. As the *fcc* of each user is different, each user uses the matrix at different levels. The method is to generate v_{32} as hierarchy parameter *fcc* in the mapping sequence:

$$\mathrm{YS} = \mathrm{Hash}_{\mathrm{Hkey}}\left(\mathrm{Alice}\right) = v_0.v_1, v_2, \cdots, v_{31}, v_{32}; \quad fcc := v_{32}$$

$$\text{Alice}_{sk} = \left(\sum_{i=0}^{31} r_{[v_i,i]}\right) \times fcc + year \bmod n = alice$$

In the numerous equivalent matrices, if a linear independent equivalent matrix is found, the equation can have a unique solution. This is an amazing new idea. Sure enough, Liao Guohong *et al.* [7] constructed an equivalent linear independent matrix with a size of 32 × 32 based on the original type of CPK, and solved the equivalent private matrix with 3000 private-keys. Thanks to the results of Liao Guohong *et al.*, It should be recognized that this is the defect of CPK, however, when the matrix was expanded to 512 × 32, the equivalent matrix method was helpless. The collusion "led" by linear dependent equation and the collusion solved by linear independent of equivalence matrix do not belong to the same concept, should not be confused.

So can the hierarchical parameter prevent linear attack of the equivalent matrix? The answer is not, because when *fcc* is a single variable, it is easy to be canceled out in elimination operation. If a number of mutually related hierarchy parameters are set up to protect each other from cancellation, the equations becomes a mixture of matrix equations and coefficient equations, whereas, the correlation of coefficient equations is obvious, which can ensure the correlation of the two equations:

$$\text{YS} = \text{Hash}_{\text{Hkey}}(\text{Alice}) = v_0.v_1,\cdots,v_{16},v_{17},\cdots,v_{32},v_{33}; \quad fcc_1 := v_{17}, \quad fcc_2 := v_{33}$$

$$Alice_{sk} = \left(\left(\sum_{i=0}^{15} r_{[v_i,i]} \times fcc_1\right) + \left(\sum_{i=17}^{32} r_{[v_i,i]} \times fcc_2\right) + year\right) \bmod n = alice$$

New things are unlikely to be mature and in the discussion on open issues, CPK has received strong support from domestic and foreign counterparts, which is the motivation for CPK to continue to take root and sprout during the decade-long ban. In 2017, it was coincided with a change of leadership of competent authority, the new leader has put an end to the mistakes of his predecessor. So CPK began to see the light.

3. CPK Smart Type

With the rise of the industrial Internet, new problems arise. Industrial internet is composed of backbone network and enterprise network. The backbone network is the global network, which mainly transmits information, while the enterprise network is the local network, which mainly transmits signals. The combination matrix of CPK original type is too large, which can only meet the information authentication requirements of intelligent terminals, but cannot meet the signal authentication requirements of non-intelligent devices. Therefore, it is necessary to design a smart CPK that can adapt to the needs of global information system as well as regional signal system.

3.1. Combination Matrix

The matrix size is defined by $h \times h$, where h is equal to 4 and 8. The private matrix ($r_{i,j}$) is kept by KMC for the generation of private-keys, while the public ma-

trix ($R_{i,j}$) is kept by each client for the computation of public-keys. The public matrix of 4 × 4 matrix and 8 × 8 matrix can be configured at the same time, or can be configured separately.

The published public matrix is signed by the Key Management Center (KMC) to determine the scope:

$$\mathrm{Hash}\left(R_{i,j}\right)_{4\times4} \to h1;\ \ \mathrm{Hash}\left(R_{i,j}\right)_{8\times8} \to h2$$

$$\mathrm{SIG}_{kmc}\left(h1\right)=\left(s_1,c_1\right);\ \ \mathrm{SIG}_{kmc}\left(h2\right)=\left(s_2,c_2\right)$$

3.2. Identifier Mapping

The mapping of the identifier to the matrix coordinates is indicated by the YS sequence, which is the output of the entity's identifier hashed under the mapping key Hkey.

$$\mathrm{YS}=\mathrm{Hash}_{\mathrm{Hkey}}\left(\mathrm{Alice}\right)=v_1,v_2,\cdots,v_k$$

YS sequence is output by bytes (8-bit), and each of three variables constitute a unit. The first two variables, v_0 and v_1, are divided into upper and lower halves, after modulo h, indicates the coordinates of row and column of the matrix, and the 0th and 1st matrix variables r_0 and r_1 are selected respectively. v_2 is taken as the hierarchy parameter *fcc*. The sum of matrix variables is multiplied by hierarchy parameters to form cell variables, such as:

$$cell_j=\left(\sum\nolimits_{j=0}\left(r_{j\times3}+r_{j\times3+1}\right)\times v_{j\times3+2}\right)\bmod n$$

$$CELL_j=\sum\nolimits_{j=0}\left(R_{j\times3}+R_{j\times3+1}\right)\times v_{j\times3+2}$$

The lower-case $cell_j$ and r_j are private-key variables, and the upper-case $CELL_j$ and R_i are public-key variables.

3.3. Key Combination

Multi Round Combination

When the matrix size is 4 × 4, the round length is 4, including 2 cell variables in one round, if operating w rounds, then

$$round_k=\left(\sum\nolimits_{k=0}^{w-1}\sum\nolimits_{j=0}^{1}cell_j\right)\bmod n$$

$$ROUND_k=\sum\nolimits_{k=0}^{w-1}\sum\nolimits_{j=0}^{1}CELL_j$$

When the matrix size is 8 × 8, the round length is 8, including 4 cell variables in one round, if operating w rounds, then

$$round_k=\left(\sum\nolimits_{k=0}^{w-1}\sum\nolimits_{j=0}^{3}cell_j\right)\bmod n$$

$$ROUND_k=\sum\nolimits_{k=0}^{w-1}\sum\nolimits_{j=0}^{3}CELL_j$$

After the multi-round transformation, the annual key is added. The annual private-key "*year*" is uniformly defined by the center, a global key, and the annual public-key is published. Year_i is a local key defined by the enterprise network.

$$Sk_{Alice} := (round + year) \bmod n$$

$$PK_{Alice} := ROUND + YEAR$$

3.4. Key Variation

Table 1 lists the relationship between multi-round of operation and variation in the case of various matrix sizes:

Thus it can be seen that the multi-round operation of the private-key expands the limited action scope to "infinite". two-round of 8 × 8 matrix is equivalent to the variation of 32 × 32 of the original CPK: $32^{32} = 1.4 \times 10^{48}$.

4. Basic Functions

4.1. Identifier Authentication

Identifier authentication is a new concept that is put forward by the logical world [8]. Nowadays, identifier is separated from identity making the concept clearer. In the physical world, the authenticity of a seal is ensured by engraved real identifier. However, there is no physical medium in the logical world, so how to ensure the authenticity of the identifier is the problem to be solved.

The identifier of the logical world is much more complex than the physical world. The identifier claimed by the subject is a phone number when connecting, the identifiers claimed by subject are IP addresses when sending packets and so on. In the logical world, there are two methods to prove the authenticity of identifier: One is the PKI certification system, in which the proof is implemented by CA certificate, where the third party CA signs to the identifier with digital signature standard DSS [9], therefore, the proof is valid only if the CA is proved to be true. The other is CPK authentication system, in which the proof is implemented by a separate identifier authentication protocol, the authentication is proven by itself.

Identifier authentication code is consisted of check code and proof code.

Check code c is the product of random number k and generator G, where x and y get through one-way function:

$$k * G = (x, y); (x + y)^2 \bmod 2^{16 \text{ or } 24} \to c;$$

Proof code s is the product of the inverse of a random number k and the private-key, if and only if there is a one-to-one mapping between the identifier and the private-key:

$$k^{-1} sk_{[\text{Alice}]} \bmod n \to s$$

Table 1. Variation under different round.

Size	Round $W = 1$	Round $W = 2$	Round $W = 3$	Round $W = 4$
4 × 4	Not Recommended	$(4.3)^2 = 1.8 \times 10^{19}$	$(4.3)^3 = 7.9 \times 10^{28}$	$(4.3)^4 = 3.4 \times 10^{38}$
8 × 8	$(64^2 \times 256)^4 = 1.2 \times 10^{24}$	$(1.2 \times 10^{24})^2 = 1.4 \times 10^{48}$	$(1.2 \times 10^{24})^3 = 1.7 \times 10^{72}$	Not Recommended

The verification is the product of the inverse of the proof code s and the public-key, if and only if there is a one-to-one mapping between the identifier and the public-key:

$$s^{-1}PK_{[\text{Alice}]} = kG \to c'$$

If $c = c'$, then the public and private keys are real, where the public-key is calculated by the verifier himself from the claimed identifier, in turn, the authenticity of the identifier is proved.

Identifier authentication is the basis of subject authentication and digital signature, but in many cases, identifier authentication is directly used as the subject authentication. The expression of Identifier authentication can be simulated as digital signature of object when object equal to zero ($h = 0$), and the authentication code is marked with $\text{SIG}_{sk\text{-}Alice}(0) = (s, c)$, and the verification code is marked with $\text{VER}_{PK\text{-}ALICE}(0, s) = c'$.

4.2. Identifier Password

Password is a common method of friend and foe identification, which is very simple and effective. It is also widely used in information systems to establish trust relation between peer entities trying to obtain subject authentication. However, with the development of cyber warfare, password has become the weakest ring. The trust established by password leads to trust-transfer, and the trust-transfer leads to the right-transfer. For example, the password causes the login success, and the successful login can obtain the right to access accounts or files. The existing passwords are fixed, unable to identify or prevent replay attack, vulnerable to DOS attack, and because the passwords are just meaningless random strings, and having the same string is not enough to prove the authenticity of subject. For this reason, some systems adopt multi-factor authentication technique, and put forward a requirement of "never trust, always verify" [10]. However, it is conceivable that multi-factor authentication will not be efficient and it will be difficult to be retained as evidence.

Identifier authentication is independent, and it also has the beforehand nature that it is always carried out before the object authentication. The independence and beforehand nature just has the characteristics that can block the trust transfer by "one thing one proof", and meets the password requirements of "evidence first, always verify". But for the replication attack, it only has the ability to identify, but does not have the ability to prevent. The identifier authentication code is changing every time under the effect of random number k, and they can only be the same if the authentication codes are duplicated. Therefore, the duplicated codes can be identified. This is the traditional symmetric password can not do, while the identifier authentication code can not only identify duplicates and but also prevent replications. But the duplicated codes can only be found by comparison, and all used codes must be registered one by one.

If the identifier authentication code is used according to a date, the comparison range can be reduced to a day, and it is feasible to find replication within a

day's registration. The following takes the date 20201123 as an example to explain the method of constructing "Identifier password":

The private key used for proof is the date added to the private key, the proof code is:

$$k^{-1}\left(sk_{[\text{Alice}]}+20201123\right)\bmod n \to s,$$

The checking code is:

$$kG=(x,y);\left(x+y\right)^2 \bmod 2^{16} \to c$$

The public key used for verification is the public key plus 20201123 * G, and the checking code is:

$$s^{-1}\left(PK_{[\text{Alice}]}+20201123G\right)=kG \to c'.$$

If $c=c'$, the verification passes.

Passwords are proved on the spot, and the date of the password is automatically provided by the terminal device. If the password is not copied on the same day, the authentication will fail. If the verification is successful, then check the replication, and records the passwords that passed authentication for the next comparison.

The authentication of identifier passwords not only prove the authenticity of the password code, but also prove the authenticity of the identifier claimed by the subject. Identifier passwords are different from traditional passwords because they are automatically derived from identifier and do not require manual input, so there is no need to remember. The password length is equal to the key length used, suitable for access information control, remote signal authentication. Copy attack is the main means of DOS attack, identifier password is an effective way to defend against DOS attack.

4.3. Digital Signature

Digital signature is the proof of the authenticity of object by subject. Therefore, a signature without a subject is not a digital signature, because there is no signer, the accountability cannot be fulfilled; and a signature with a subject but not authenticated, it's not a digital signature either, because the subject can be counterfeited and cannot be used as evidence. In PKI certification system, the signer has a private-key and the verifier obtains the public-key from LDAP, which is certified by a third-party CA, whereas a public key is proven to be someone's, so if the public- and private-keys are paired, the authenticity of the public key and identifier,are proved, and it can be regarded as a digital signature If the third-party CA's authenticity can be certificated, However, if the third-party CA's authenticity cannot be certificated, it cannot be regarded as a real digital signature.

While under the evidence based authentication logic, a signature can only be established on the basis of identifier authentication. Because only the authenticity of the identifier of subject has been proved, can it be qualified to provide au-

thenticity proof for the object. Therefore, the proof of identifier authenticity must be included in every signature. It needs the DSS of trust-based logic to be interpreted in a new way of evidence-based logic.

Signature code consists of proof code and check code.

Check code c is the product of random number k and base point G to get through one-way function variation:

$$kG = (x, y); (x + y)^2 \bmod 2^{16 \text{ or } 24} \to c ;$$

Proof code s is the sum of the identifier proof code and object proof code:

$$\left(k^{-1}h + k^{-1}sk_{[\text{Alice}]}\right) \bmod n \to s$$

Where h the feature of an object. The signature function is marked by

$$\text{SIG}_{sk\text{-}alice}(h) = (s, c)$$

The verification is the sum of identifier check code and object check code:

$$s^{-1}hG + s^{-1}PK_{[\text{Alice}]} = kG \to c'$$

Object verification code is the object h and G are multiplied, so that h and hG form a public- and private-key pair. If $c = c'$, then the authenticity of identifier and object is proved. Because the public-key used is calculated by the verifier himself from the identifier claimed by the subject, it first proves the authenticity of the identifier of subject, and then proves the authenticity of the object with the verified identifier, so the signature is valid. The verification function is marked by $\text{VER}_{PK\text{-}ALICE}(h, s) = c'$.

There are three forms of object existence in digital signature: ontology, slave and target. When the feature of object h is ontology, the signature is the proof of traceability evidence; when h is the feature of slave, the signature is the attribution evidence; when h is the feature of a target, the signature is the responsibility evidence.

The characteristic of digital signature is that a signature proves the authenticity of both the subject and the object simultaneously. Digital signature is used to prove the authenticity of entities and of events. Where the authenticity of the event is divided into the accept process and the adopt process, called ex-ant authentication and ex-post authentication. In some cases, the two processes need to be processed separately. For example, in communication, it is needed to verify the validity of the communication before receiving data to prevent illegal access. The object may be a composite entity, which can be signed individually or signed only once for the composite entity, for example:

$$\left(k^{-1}(h_1 + \cdots + h_n) + k^{-1}sk_{[\text{Alice}]}\right) \bmod n \to s$$

Authentication system is an evidence-based proof system that integrates evidence-showing and verification. Evidence provides the basis of verification. Without evidence, verification has no basis. Therefore, the evidence-showing system is the active side, and the verification system is the passive side. The perfection of the authentication system depends on the completeness of the evidence-showing

system. Digital signature is the core technology of the evidence-showing system because most of the evidence is provided by digital signature.

4.4. Key Encryption

Key encryption protocol is as follows:

Suppose that Alice sends a encrypted data to Bob: Alice first selects a random number r to calculate the data encryption key:

$$r*G=\text{key}$$

Encrypts the data with the key

$$\mathrm{E}_{\text{key}}(\text{data})=\text{code}$$

Alice calculates Bob's public-key *PK-BOB*, and encrypts the data encrypting key with the public-key:

$$r(PK\text{-}BOB)=\beta$$

Key encryption is marked with $\mathrm{ENC}_{PK\text{-}BOB}(\text{key})=\beta$. Alice sends (code, β) to Bob.

Bob decrypts the key with his private-key:

$$\beta(sk\text{-}bob)^{-1}=r*G=\text{key}$$

Key decryption is marked with $\mathrm{DEC}_{sk\text{-}bob}(\beta)=\text{key}$. Bob decrypts the data with the key:

$$\mathrm{D}_{\text{key}}(\text{code})=\text{data}.$$

Key management is the core issue of encryption system, the main task is to create a network that can be closed or opened flexibly. Identifier-based keys bring great convenience to key management, because the public-keys are calculated by the users, so the encrypted communication between any two points can be realized on the public network, reducing the granularity of segmentation from the LAN to the communicating two sides, without the need for additional regional segmentation. However, when a closed secure network is needed, the annual key year1 is set for LAN, so that the whole network can be connected with the annual key Year, ensuring only to be connected within the private network with annual key year1. When the same encrypted message needs to be distributed to several people, it only needs to encrypt the key with the public key of different people. Identifier-based keys in different service can naturally be classified according to different identifiers, no artificial classification of keys is required. No artificial classification of keys is required. Encryption on the public network only needs to meets the requirement of turning secret files into public files. Because data encryption keys are encrypted with public keys, they can also be stored or sent publicly.

5. Summary

After 20 years of development, CPK is still the most simple system that can solve

identifier authentication, identifier password, digital signature and key encryption. Where identifier authentication is the basis of digital signature, and only on the basis of identifier authentication can a digital signature be constructed. Digital signature provides evidence of authenticity, traceability, attribution and responsibility, and is the core technology of maintaining Internet order. The signature system of CPK provides a technical basis for the creation of truth logic of authentication [11], which sublimates the traditional authentication logic based on trust to the logic based on evidence, and provides a technical basis for the construction of a GAP universal authentication protocol [12], which elevates the traditional multi-step proof protocol to one-step direct proof protocol.

In the physical world, most of the evidence is provided by seals, and in the logical world, by digital signatures. Digital signature has incomparable advantages over physical seal, and the emergence of two-dimensional code makes digital signature to be digital seal, which is universal in the physical world and the logical world. Therefore, identifier authentication and digital signature will play an important role not only in the logical world, but also in the physical world. It will lead to a new situation where authentication techniques can be used in both the physical and logical worlds.

The arrival of the quantum age raises new problems for the research of digital currency, because the money issued now must still be valid in the quantum age. Under the existing signature protocol, public-keys must be open to the verifier, and public-keys cannot resist quantum exhaustion. Therefore, we can only seek a new way that even a public key is broken, it does not have any significance, therefore, CPK time type has been designed adopting one-time signature mechanism, which is easy to detect the crime using the cracked private-key.

Internet is a great invention, the common wealth of mankind and a platform for the exchange of human wisdom. Maintaining order on the Internet is the common responsibility of every user. Through the study of CPK, it is seemed to have seen a bit of hope, and expected a common effort of colleagues to promote the development of cyber security.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Shamir, A. (1984) Identity-Based Cryptosystems and Signature Schemes. *Advances in Cryptology*, **21**, 47-53. https://doi.org/10.1007/3-540-39568-7_5

[2] Nan, X.H. and Chen, Z. (2003) Profile to Network Security. Publishing House of Defense Industry.

[3] Yu, M.Y., Huang, X.P., Jiang, L., *et al.* (2008) Combined Public Key Cryptosystem Based on Conic Curves over the Ring Zn. 2008 *International Conference on Computer Science and Software Engineering*, Wuhan, 12-14 December 2008, 631-634. https://doi.org/10.1109/CSSE.2008.542

[4] (2000) Standard for Efficient Cryptography. SEC1: Elliptic Curve Cryptography.

[5] (2000) Standard for Efficient Cryptography. SEC2: Elliptic Curve Cryptography.

[6] Nan, X.H. (2021) New Progress in CPK Public Key. *Open Access Library Journal*, **8**, 1-6. https://doi.org/10.4236/oalib.1107440

[7] Liao, G.H., *et al.* (2016) linear Collusion Attack to CPK, Computer Application and Software.

[8] Nan, X.H. (2006) CPK Identifier Authentication. Publishing House of Defense Industry.

[9] (1994) Digital Signature Standards, National Institute of Standards and Technology. NIST PUB 186, U.S. Department of Commerce.

[10] Department of Defense (DOD) (2021) Zero Trust Reference Architecture, Version 1.0.

[11] Nan, X.H. (2020) CPK Solution to Cyber Security Theory and Practice, Chapter Three CPK Truth Logic. Publishing House of Electronics Industry.

[12] Nan, X.H. (2020) GAP One-Step Authentication Protocol, Communication Technologies, Vol. 53.