Research on Zero-Knowledge Proof Protocol

Wang Huqing[1,2], Sun Zhixin[3,4]

[1]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China
[2]College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing,China
[3]College of Internet of Things , Nanjing University of Posts and Telecommunications, Nanjing, China
[4]State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, China

Abstract

Zero-knowledge proof protocol is a critical component of cryptography, which in recent years has raised increasing concern of many scholars.Its application field is very extensive,and it has made breakthrough progress in many aspects,including mathematics and network safety and so on. This article launches the elaboration from the concept, nature, mathematics theory, general proof process of the zero-knowledge proof , focusing on the application research of polynomial function root, graph isomorphism, cloud storage service, RFID, proxy digital signature and identity authentication etc.Finally, the direction for further research is summed up.The systematic introduction to zero-knowledge proof protocol has important theoretical guidance and practical significance on attracting more scholars involved in the research as well as expanding application fields.

Keywords:zero-knowledge proof; identity authentication; digital signature; cloud storage; polynomial function root

1. Introduction

Zero-knowledge proof ,a very interesting and important applicative topic[1]，which has attracted a lot attention of peer scholars, having achieved abundant achievements in many security related fields , has became one of the hot issues in the research fields of cryptography[2][3].

1.1 Main ideas

The main idea of zero-knowledge proof is as follows: P (the prover) had some secret information. P wanted to prove to V (the verifier) by taking other proof process without revealing anything other than the fact that it knows in order to prevent the confidential information from leaking to anyone (including V or any other third party). We call this technology which can achieve the purpose of proof without revealing anything " zero-knowledge proof(ZKP) "[4].

1.2 Example analysis

Nineteen eighties, Goldwasser et al first put forward the concept of zero-knowledge proof [5]. We can understand the zero- knowledge proof from the case in life:

(1) Supposing a room can only be opened by a key with nothing else available,The prover P wanted to prove himself owning the room key without revealing the key to the verifier V to prevent leakage. Therefore, if V determined that the room had a certain object, P can take out the object to prove himself having the key. This proof process is zero-knowledge proof, and " knowledge " is the key [6].

(2) zero-knowledge proof of color blind with red and green ball[7]

Surpposing the verifier V is color blind.There are now two balls,one is red, another is green.The two balls are exactly the same besides their color.It is required to prove to V that the two balls are truly different because they seem to be identical to him. We adopt the following method: let V hold a ball in each hand, standing opposite P. P can also see this two ball without telling V which is red and which is green. Then, let him take hands behind his back, he can decide randomly whether to swap the balls or not. The probability of exchanging or not each accounted for 1/2. Finally, he takes balls from back and asks P to answer whether V has exchanged two balls. According to the color of the ball, P can simply judge. Repeatedly, if P can answer correctly everytime, then V will believe that these two balls color are different to a large enough probability . The process also belongs to zero-knowledge proof, and " knowledge " is the color of the ball.

(3) The most typical example of zero-knowledge proof is the Cave model which was put forward by Jean-Jacques Quisquater and Louis Guillou[7]. As shown in Figure 1:

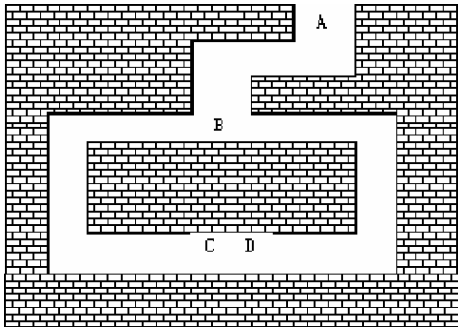

Fig.1 : the cave model.

1.3 the general process of zero-knowledge proof protocol

The general process of using zero-knowledge proof protocol is shown in following figure:

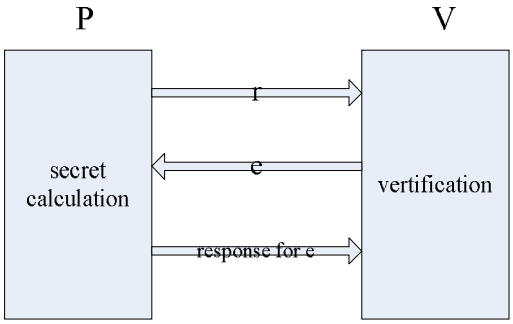

Fig 2:the general process of zero-knowledge proof protocol

(1)The prover P sents promise random number r to the verifier V.
(2)V sents random challenge value e to P.
(3)P calculats secretly and sents the result to V as the challenge-response for second step.
(4)V verifies the response. If the verification fails, the process of proof will end.Otherwise, the above steps will be repeated for N times. If every verification can be successful , V will receive P's proof in great probability.

1.4 Nature of zero-knowledge proof protocol

Zero-knowledge proof protocol has the following three important properties.In other words, using zero-knowledge proof protocol to prove a problem, the proving system must meet the following requirements:
(1) Completeness
If the prover P and the verifier V comply with the general process of zero- knowledge proof protocol strictly, the proof is considered to be successful and P is credible.
(2) Rationality
If it failes once in N times of verification,the proof is regarded as failed and P is a fake prover who is unreliable.
(3) Zero-knowledge
During the verification,V can't obtaion any privacy or important information,let alone anything about the knowledge,except to believe that P dose have it.Even though V verifies repeatly,he can not prove the existing fact to others anymore.

2.Key mathematical knowledge applied to zero-knowledge proof protocol

The commonly used algorithm theory in zero-knowledge proof , which is similar to public-key cryptosystems in cryptography ,is mainly based on the following key mathmetic problem:
(1)the square root problem of modulo n
Given a positive integer n , a∈Zn, if there exists x∈Zn that makes x2=a(mod n), then x is called as a square root of modulo n.
(2) the calculation problem of the discrete logarithm
Given a prime number p,and a,which is one of the primitive element on finite field Zp .To b on Zp,looking for one and only integer c that makes a^c≡b(mod p). In general, the problem is difficult if you are looking forward p, and there is still no algorithm to calculate polynomial of discrete logarithm. The method based on the elliptic curve discrete logarithm is commonly used.
(3) Large integer factorization problem
The factorization of a large integer M which is N digit, is usually impossible to be done in O (N) , but rather to up to O (exp (N)) level.

3. Typical application and Implementation of zero-knowledge proof protocol

3.1 Zero-knowledge proof of polynomial function root

Assuming that P has got a solution x0 to an integral coefficient high-order polynomial function f (x), he wants to prove himself without revealing x0 or any information about x0 to V.This is a zero-knowledge proof problem of polynomial function root . In document [8], the author introduces multiple discrete logarithm problem and puts forward zero-knowledge proof algorithm of polynomial function root , on the basis of solving problem of discrete logarithm.
Assuming integral coefficient high-order polynomial function $f(x) = \sum_{i=0}^{n} a_i x^i$, the process is shown as follow:

(1) prover P and verifier V choose p and generating element α of Z_p^*

(2) P calculates $\beta_i = \alpha^{x^i} \bmod p, i = 1,2,\cdots n.$ and sends the result to V

(3) P proves himself having the solution x_0 to establish $\beta_i \equiv \beta_{i-1}^{x_0} (\bmod\ p), i = 1,2,\cdots n$ to V by using zero-knowledge proof method of multiple discrete logarithm.

(4) V verifies $\prod_{i=0}^{n} (\beta_i)^{\alpha_i} \equiv 1 (\bmod\ p)$

The above process is repeated many times.

3.2the Isomorphism problems

Assuming there are 2 undirected graphs G1=<V1，E1> and G2=<V2,E2> , the number of their vertices are equal and the number of their sides are equal .If there exists a replacement, φ ,which makes any （u，w）∈E1 meet φ （u，w)∈E2 , the two graphs are isomorphic. If P wants to prove that it knows the replacement φ ,which satisfies the conditions while P does not want to disclose any relevant information ,it is a zero-knowledge proof problem.

The proof is given in the literature [9]:

(1)P randomly selects a replacement γ , in the role of γ , converts Figure G1 into Figure H and sends it to V .

(2)V randomly selects e∈{0,1} and sends it to P .

(3)P calculates based on the value of e ,if e=0， sends $\pi = \gamma$ ； if e=1,sends $\pi = \gamma\ \varphi$ -1

(4)V Verifies whether H= π Ge is established .

The above process is repeated many times.

3.3 Cloud storage services security management

The security, reliability, and availability of cloud storage services are the important factors which result in the widely uses of the cloud storage business .In order to obtain the user's trust, the cloud storage service provider must provide the users with recoverability proofs(POR，a proof of retrievability)[10],and prove the integrity and security of the data.Considering the security of POR protocol , there are mainly two points which are listed as following :

(1)How to prevent prover from deceiving the verifiers by tampering data in the process of verification ?

(2)For publicly verifiable POR protocol , how to prevent malicious verifier to store data by analyzing the response of public challenges?

Based on the above two security issues ,in the POR protocol ,we can consider using the zero-knowledge proof .The completeness and rationality of the zero-knowledge proof method can ensure the security of the first point and the “zero-knowledge” characteristic of the zero-knowledge proof method can ensure the security of the second point .

In the literature [11], the author suggests the zero-knowledge data recoverability proof protocol model, which can prevent the provers` deception and the leak of validation data . The certification process is in strict accordance with the process of Figure 2 mentioned above.The algorithm mainly uses the bilinear map group system S=（p,G,GT,e) where G and GT of two large prime numbers p-group of order and will need to verify that the data file F into a partition F= $\{m_{i,j}\} \in Z_p^{n\times s}$, the secret data of each sub-block $\{m_{i,j}\}$ is protected by the random number $\lambda_j \in Z_p$ and tag $\{\sigma_i\}$ is protected by the random number $\gamma \in Z_p$ .Moreover to avoid malicious verifier from obtaining $\{\lambda_j\}$ and γ , the author takes advantage of a committed method to protect by using H_1^{λ} and $e(\prod_{i=1}^{s} u_i^{\lambda_i}, H_2)$ where $H_1 = h^{\alpha}$, $H_2 = h^{\beta}$, α and β are random numbers of $\in_R Z_p$; h is an anti-collision Hash function， $u_i = g^{\tau_i} \in G$, τ_i is a random number which $\in Z_p$ and its range:（i=1,⋯ s), E is the mapping of the bilinear map group system .

3.4 Applications in the RFID

RFID(Radio Frequency Identification) is mainly composed of the readers, tags and databases.Since there are enough energy and computing resources between the database and the reader ,traditional cryptographic algorithms can be considered in terms of safety , it is commonly believed that the passage between the two is secure . But the communication media between the reader and the tag is a wireless media ,which is completely exposed to the attacks and other unauthorized readers . The transfer of information lacks confidentiality and there is a possibility of malicious attacks.For example, an attacker can replay legitimate reader or tag signal to counterfeit in order to get the trust of the label or reader . Thus the attacker obtains secret information .To be against such attacks, to verify the identity of a legitimate

reader or tag and not to disclose any private information is especially important . To achieve the purpose of proving legal identity without disclosing any private information ,scholars have thought of using zero-knowledge proof protocol to deal with the problems.In the literature [13] and [14] ,the author shows the mutual authentication protocol based on zero-knowledge proof protocol RFID which are between the reader and tags . Here, we can give out the zero-knowledge authentication method based on the reader of elliptic curve . Fig.3:

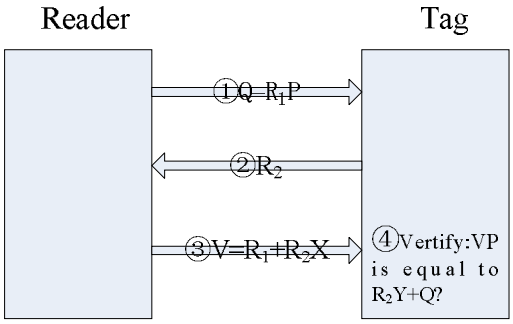

Fig.3: zero-knowledge proof protocol applied in RFID

The algorithm principle of this authentication is to use the elliptic curve to deal with discrete logarithm problems .Here is an introduction of the parameters related to what mentioned above:

① Finite field selection GF(2m)； parameters a and b，define the elliptic curve

E: $Y^2 = X^3 + aX + b(p > 3)$ or

$Y^2 + XY = X^3 + aX + b(p = 2)$

② P denotes the basis point

③X is the private key，Belong to the random intervals in the range of [1.n-1]； Y is the public key， Y=XP

④ R1 and R2 are both random integers，and R1∈[1,n-1]，R2≥1.

3.5 proxy digital signature

Currently， the two most popular public-key digital signature methods ： one is the RSA digital signature method which is based on the decomposition of large factor difficult ， and the other is the ELGamal type digital signature method which is based on the finite field GF (p) looking for discrete logarithm difficult . The proxy signature is needed when the real signer is absent .It is neither feasible nor safe to obtain the real signer's private key in computing.So,the common solution is to produce proxy signature ,but not the proxy signer .Proxy signature has the following properties :

① The dissimilarity between Proxy signature and normal signature，

② The Unforgeability. Only the original signer and designated agent signer can produce effective proxy signature，

③ Verifiability .Judging from the proxy signature ,the validators can believe the original signer identity the signature news ，

④ Identifiability. The original signer can recognize the identity of the proxy signers from the proxy signature.

⑤ Non-repudiation. The proxy signer cannot deny the proxy signature which was erected and approved by himself.

Based on the requirements above and the characteristics of zero-knowledge proof, we can consider using zero-knowledge proof agent agreement principles to realize the Proxy Digital Signature. Literature [15][16][17] all put forward specific ways which use zero-knowledge proof agent agreement to realize the Proxy Digital Signature.The literature [15] is based on the problems of computing discrete logarithm.By using zero-knowledge digital signatures ,it puts forward not only a proxy signature scheme ,but also a multiple proxy signature scheme .These two scheme can effectively prevent the original signer from faking the proxy signer and forging proxy signature key for proxy signature .The literature [16] puts forward a zero-knowledge digital signature scheme based on RSA，but the zero-knowledge proof agreement in literature [16]continues using the first Fiat - Shamir identity authentication protocol process.In literature [17],it indicates that by using the zero-knowledge proof thoughts ,we can prevent others from faking the infomation owner to ask the proxy signers for the signature.In the following fig.4 ,it shows the algorithm flowchart of the realization of proxy signature by using the zero-knowledge proof.

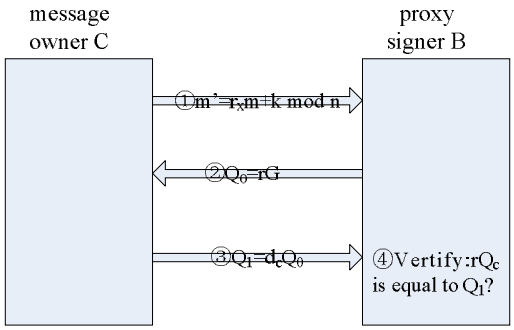

Fig.4: Zero-knowledge proof protocol applied in proxy digital signature

The principle of the algorithm is also calculated based on the problems of the elliptic curve discrete logarithm. The

parameters related to what mentioned above are as follows :

①Let Fq be a finite field with Q elements, E is the elliptic curve ;

② Set G as a base, n is the order of G;

③ k is a random integer in the range of [1, n - 1], R = kG = (rx, ry), m '= RxM + k mod n, m R is the information of the signature ;

④ r is a random integer in the range of [1, n - 1] , Q0=rG ;

⑤dc is the private key of the message owner C， Qc is the public key of C , Qc=dcG.

3.6 Identity Authentication

If "zero-knowledge" means identity information, then zero-knowledge proof protocol can be applied to identity authentication.The common authentication requires transmission of password or personal secret information ,which will give attackers loopholes to attack more or less[18][19]. With zero-knowledge proof of identity , one can prove himself legal to the system without transfering above information .There are large amounts of documents show that zero-knowledge proof protocol has great superiority and importance in the field of authentication presently[20][21][22][23]. Fiat-Shamir authentication is the first that had been proposed, while it is the most basic zero-knowledge authentication scheme. The process of Fiat-Shamir authentication is shown in fig.5:

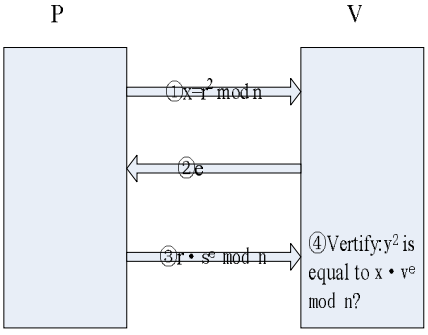

Fig.5: Fiat-Shamir authentication process

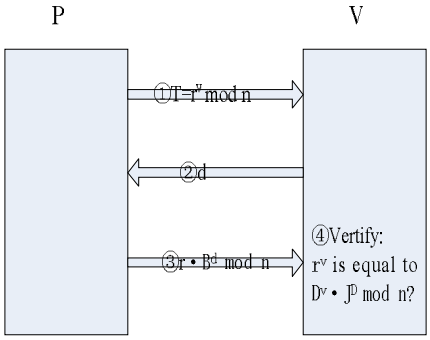

Fig.6: Guillou-Quisquater authentication process

The introduction of the parameters about Fiat-Shamir authentication process :

① n= $p \times q$,n is a random modulus , p and q are two large primes.

② s is the private key of the prover P . v is the public key of P . s and n are coprime. $v = s^2 \bmod n$

③ r, a committed random number,is a random integer,which ∈[1,n-1].

④ e∈{0，1},a challenging bit.

In addition, we give the Guillou-Quisquater authentication, a classic authentication process. The process of the Guillou-Quisquater authentication is shown in figure 6:

The introduction of related parameters :

①J，v，n are public keys , n= $p \times q$, p and q are two large primes.

②B is the private key ,which meets $J \times B^v = 1 \bmod n$.

③ r, a committed random number,is a random integer,which ∈[1,n-1].

④ d∈[0,v-1], a challenging bit .

4 Conclusions and prospects

zero-knowledge proof protocol has become a very important component in cryptographic algorithms and security protocols.In this paper,the main idea,nature, general proof process, mathematical theory and specific applications of zero-knowledge proof protocol are introduced.Zero-knowledge proof protocol has the advantage of zero leakage proof, so it can be applied to prove many key issues,like many classic mathematical problem: the polynomial function roots, the graph isomorphism,as well as other NP problem[24], such as the Sudoku games [25]. The prover can prove that he has the method to solve some problem and he does not worry about the method revealed. Zero-knowledge proof

protocol are very useful in the field of network and information security too,like authentication, digital signatures, etc.It is very important that proving to each other the identify of the user without revealing the user information in authentication and digital signatures.In order to effectively prevent unauthorized users impersonating legitimate users,we can use zero-knowledge proof protocol to authenticate.

Research on a large number of documents, we can see that during the process of zero-knowledge proving,it must meet its three nature including completeness,rationality and zero-knowledge and the procedure must follow the steps of Fig. 2.

In our future study,we will focus on using zero-knowledge proof theory to solve more problems and exploring its broader applications.In this paper,for many applications,some simple proof algorithm and process is given, the calculation of mathematical formula and the details of the proving procedure are not given explanation in-depth,the complexity of communication and computation is not considered yet.All those will be the content of our next task.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under Grant(No. 60973140, 61170276), the National High Technology Research and Development Program of China (863 Program) (No. 2009AA01Z212),the Natural Science Foundation of Jiangsu Province under Grant(No.BK2009425),the construction project of Jiangsu Province advantage discipline " Information and Communicaiton Engineering",the research project of Nanjing University of Posts and Telecommunications(No. NY210034).

References

[1]Lindell,Y;Zarosim,H.Adaptive Zero-knowledge Proofs and Adaptively Secure Oblivious Transfer.[J].Journal of Cryptology.24(4),pp.761-799,2011

[2]Garg,Sanjam;Jain,Abhishek;Sahai,Amit.Leakage-resilient zero knowledge.31st Annual International Cryptology Conference,CRYPTO 2011.pp:297-315.

[3]Lin,Huijia;Pass,Rafael;Tseng,Wei-Lung Dustin;Venkitasubramaniam,Muthruamakrishnan.Concurren t non-malleable zero knowledge proofs. 30th Annual International Cryptology Conference,CRYPTO 2010.pp:429-446.

[4]Bayer,Stephanie;Groth,Jens.Efficient zero-knowledge argument for correctness of a shuffle.31st annual International Conference on the Theory and Applications of Cryptographic Techniques,EUROCRYPT 2012.pp:263-280.

[5] S.Goldwasser,S.Micali,C.Rackoff.The Knowledge Complexity of interactive Proof Systems.Proceddings of the 17th ACM Symposium on Theory of Computing 1985,291-304.

[6] http://baike.baidu.com/view/1228083.htm.

[7]Zhang Yinbin. Research on Zero-Knowledge Proof and Its Applications[D].China:Huaibei Normal University,2011

[8]Li Xi,Wang Daoshun.Zero-knowledge proof protocol of the roots of polynomial functions[J].Journal of Tsinghua University(Science and Technology),2009,Vol.49,No.7,pp:999-1002.

[9] Goldreich O,Micali S,Wigderson A.Proofs that yield nothing but their validity and a methodology of cryptographic protocol design [J].FOCS,1986.174-187

[10Juels A,Kaliski-Jr B S.Pors:Proofs of retrievability for large files.In:Proceedings of the 2007 ACM Conference on Computer and Commnunications Security,CCS 2007.Alexandria:ACM,2007.584-597.

[11] Zhu y;Wang HX;Hu ZX;Ahn,GJ;Hu,HX.Zero-knowledge proofs of retrievability.Science China-Information Sciences.54(8),pp.1608-1617,2011.

[12]Huang,YJ;Lin,WC;Li,HL.Efficient Implementation of RFID Mutual Authentication Protocol.IEEE Transactions on Industrial Electronics.59(12),pp.4784-4791.2012.

[13] Liu,H;Ning,HS.Zero-Knowledge Authentication Protocol Based on Alternatiove Mode in RFID Systems.IEEE Sensors Journal.11(12),pp.3235-3245,2011

[14]Wang Xiao-mei,Zhang Qiu-jian.Mutual Authenticantion for RFID based on elliptic curve and zero knowledge[J].Computer Engineering and Applications.pp:1-4,2012.

[15]Tan Zuo-wen,Liu Zhuo-jun.Proxy Signature Schemes Based on Signature of Zero-Knowledge[J].Computer Science.Vol.31,No.11,pp:70-72,2004.

[16] Qi,CM;Cui,SM.A Zero-Knowledge Proof of the RSA Digital Signature Scheme.1st International Symposium on Computer Network and Multimedia Technology.Vol(1and 2),pp.1037-1040,2009

[17]Zhang Jian-zhong,Ma Wei-fang.Blind Proxy Blind Signature Scheme on Elliptic Curve[J].Vol.36,No.11,pp:126-127,2010.

[18]Upadhyay,Saurabh;Singh,Sanjay Kumar.Video Authentication:Issues and Chanllenges[J].International Journal of Computer Science Issues.Vol.9,No.1-3,pp:409-418,2012.

[19]Malempati,Sreelatha,Mogalla,Shashi.Enhanced authentication schemes for instruction prevention using native language passwords[J]. International Journal of Computer Science Issues.Vol.8,No.4-1,pp:356-362,2011.

[20] Jaafar,Abdullah M;Samsudin,Azman.Visual zero-knowledge proof of identity scheme:A new approach.2nd International Conference on Computer Research and Development.pp.205-212,2010.

[21] Naranjo,JAM;Antequera,N;Casado,LG;Lopez-Ramos,JA.A suite of algorithms for key distribution and authentication in centralized secure multicast environments.[J].Journal of Computaional and Applied Mathematics,236(12),pp.3042-3051,2012

[22] Camenisch,J;Gro,T.Efficient Attributtes for Anonymous Credentials.ACM Transactions on Information and System Security.15(1),SI(4),2012.
[23] Chang Qing,Zhao Fang.Research of Authentication System Based on Zero-knowledge Proof[J].Value Engineering,pp:167,2010.
[24] Minh-Huyen Nguyen;PSalil Vadhan.Zero knowledge with efficient provers.Poceedigns of the thirty-eighth annual ACM symposium on Theory of computing.pp,287-295,2006
[25] Chien,Yu-Feng; Hon,Wing-Kai.Cryptographic and Physical Zero-Knowledge Proof:From Sudoku to Nonogram.5th International Conference on Fun with Algorithms.Vol(6099), pp:102-112,2010.

Wang Huqing received master degree from Nanjing University of Posts and Telecommunications in 2004.She has been worked in her home university since 2004. Now,she is pursuing the PHD degree in the field of network security under the guidance of Dr.Sun Zhixin in Nanjing University of Aeronautics and Astronautics

Sun Zhixin has around twenty years both teaching and research experience.He is the leader of College of Internet of Things in Nanjing University of Posts and Telecommunications and he is the editor of many journal like computer communication,Journal on Communication ,Journal of Software and so on.