The Trusted Two-dimensional Code System based on Certificate-based Signature Scheme

Tianhan Gao*, Luoyin Feng, Yingnan Zhao, Shiyue Qin, and Quanqi Wang
Department of Software College, Northeastern University, No.11
the 3rd Lane,Wenhua Road, Heping District, Shenyang, 110819, China
gaoth@mail.neu.edu.cn, 448501751@qq.com, 875317394@qq.com,
qsy_ghost@163.com, wqq_7622@126.com

Abstract

With the high capacity, fast recognition speed, as well as strong correction ability, two-dimensional code is widely used in many fields such as e-commerce. However, how to guarantee the authenticity of two-dimensional code becomes an urgent security demand. In this paper, we design and implement an authentic two-dimensional code system based on certificate-based signature scheme (CBS). The system includes trusted center module, authentic two-dimensional code generation module, and authentic two-dimensional code verification module. The trusted center is in charge of initializing system parameters and issuing certificates. Two-dimensional code generation module achieves secret key reading from USBKey and two-dimensional code generation functions. Two-dimensional code verification module is responsible for two-dimensional code scanning and CBS signature verification. Bilinear pairing is adopted to implement the CBS algorithms. The web interface is built with JavaScript. Further productization of the prototype system will play an important role in promoting secure application of two-dimensional code.

Keywords: Two-dimensional Code,authentication,Certificate-based signature,USBKey

1 Introduction

Nowadays, two-dimensional code has become more and more popular and is widely used in public places such as theaters, cafeteria and so on. At the same time, the security issues of two-dimensional code also draw a lot of attentions since the content of two-dimensional code may contain some malicious link which can result in further threats to end users.

For the security of the two-dimensional code,Yu Xiao yang[9] etc. utilize the traditional ECA (Elementary Cellular Automata),Qingbo Kang[5] etc. adopt the chaotic encryption to solve the confidentiality of two-dimensional code respectively. However, these proposals only address the confidentiality of two-dimensional code while no concern for its authenticity. Cátia Santos-Pereira[7] guarantee the authenticity of two-dimensional code based on PKI (Public Key Infrastructure), while the heavy maintenance and processing load restrict the practicality of the scheme. In sum, the literature research of trusted two-dimensional code are subject to their security, adaptability, as well as efficiency.

In this paper, we design and implement a trusted two-dimensional code system based on Certificate-based signature(CBS) scheme from the authenticity point of view. The system integrates CBS into the generating and the scanning procedures of two-dimensional code in order to protect the legal interest of merchants and consumers during their usage of two-dimensional code.

Research Briefs on Informaiton & Communication Technology Evolution (ReBICTE), Vol. 1, Article No. 14 (January 15, 2015)

*Corresponding author: Department of Software College, Northeastern University, No.11, the 3rd Lane, Wenhua Road, Heping District, Shenyang, 110006, China, Tel: 8624-83681822

The rest of this paper is organized as follows. Section 2 introduces the preliminaries of CBS and two-dimensional code briefly. Section 3 is the design and analysis of our trusted two-dimensional code system. The implementation of the prototype of our system is elaborated in Section 4. Finally, we conclude the paper in Section 5.

2 Related Technology

2.1 Bilinear pairing

Let G_1, G_2 be two additive cyclic groups of same prime order p and let G_T be a multiplicative cyclic group.
A mapping $e : G_1 \times G_2 \to G_T$ which satisfies the following properties is called bilinear paring:
(1) Bilinear: For all $P \in G_1, Q \in G_2$ $a, b \in Z$, the equation $\mathrm{e}(aP, bQ) = \mathrm{e}(\mathrm{P}, Q)^{\mathrm{ab}}$ is always right.
(2) Non-degenerative: There exits $P \in G_1, Q \in G_2$ which can make $\mathrm{e}(P, Q) \notin 1 \in G_T$ always right.
(3) Computability: There is an efficient approach to work out the result of e in accessible time.

2.2 Certificate-based signature scheme

Kang etc. suggested the CBS[4] [6] [1] based on Certificate-based encryption (CBE[2]) including the following algorithms.
Setup: CA generates two groups G_1, G_2 with same order q and a bilinear pairing $e : G_1 \times G_1 \to G_2$. Choosing a Generators $P \in G_1$ and a random key $s_C \in Z_q^*$ and computing the system public key $PK_C = s_C P$. Meanwhile, choosing two key hash function $H_1 : \{0,1\}^* \to G_1$ and $H_2 : \{0,1\}^* \times G_1 \to Z_q^*$. After System parameters are initialized, the system parameters$(G_1, G_2, e, q, P, PK_C, H_1, H_2)$ are published.
UserKeyGen: Users choose their own private key $s_A \in Z_q^*$ randomly, compute their own public $PK_A = s_A P$, and the user's public and private key pair are (PK_A, s_A).
CertGen: Users send their own identity information to CA. The identity information includes their own public key $PK_A = s_A P$ and some necessary information to verify their identity like the ID. CA verifies users'information. If valid, then computes $P_A = H_1(PK_C || PK_A || ID_A) \in G_1$, and generates the certificate $Cert_A = s_C P_A$, finally sends the certificate to users.
SignKeyGen: To sign the message, the signer computes the temporary signing key $S_A = s_C P_A + s_A P_A^{'} = Cert_A + s_A P_A^{'}$ where $P_A{}^{'} = H_1(PK_A || ID_A) \in G_1$.
Sign: For the message M to be signed, signer chooses a random $r \in Z_q{}^*$, and then computes the signature $\sigma = (U_1, U_2, V)$ and $U_1 = rP_A, U_2 = rP_A{}^{'}, V = (r+h)S_A = (r+h)(s_C P_A + s_A P_A{}^{'})$ where $h = H_3(M, U_1, U_2)$.
Verify: When the verifier gets the signature σ, checks if the equation $e(PK_C, U_1 + hP_A)e(PK_A, U_2 + hP_A^{'}) = e(P, V)$ holds to verify whether the signature σ is valid and outputs a binary value 0 (invalid) or 1 (valid).

2.3 Two-dimensional code

Two-dimensional code is a graphical image that stores information both horizontally and vertically, and utilizes optical scanning equipment to get the information automatically[3]. Two-dimensional code can be divided into two categories: stacked two-dimensional code and matrix two-dimensional code. Stacked two-dimensional code includes PDF417, Code 49, Code 16K and etc. Matrix two-dimensional code contains Code one, Aztec, Date Matrix, QR code and etc. QR code is short for quick response matrix, which is composed of square, blank area, functional graphics area, and data graphics zone. The system in this paper is mainly designed for QR code.

3 Trusted two-dimensional code system

3.1 System Architecture

As shown in Figure 1, the trusted two-dimensional code system includes trust center (TC), merchants and users. TC is the trusted root of the system, and mainly responsible for confirming merchant's identity and issuing the CBS certificate to merchant. The modules need to be implemented are: merchant registration module, merchant certification module, as well as CBS certificate issuing module. Merchant is mainly responsible for releasing credible two-dimensional code and applying certificate from TC. The related modules are: public and private key generation module, certificate applying module, signing key generation module, and two-dimensional code generation module. User, primarily responsible for installing the scanning software on the smart phone for scanning and verifying the two-dimensional code. The corresponding module is two-dimensional code scanning and verifying module.

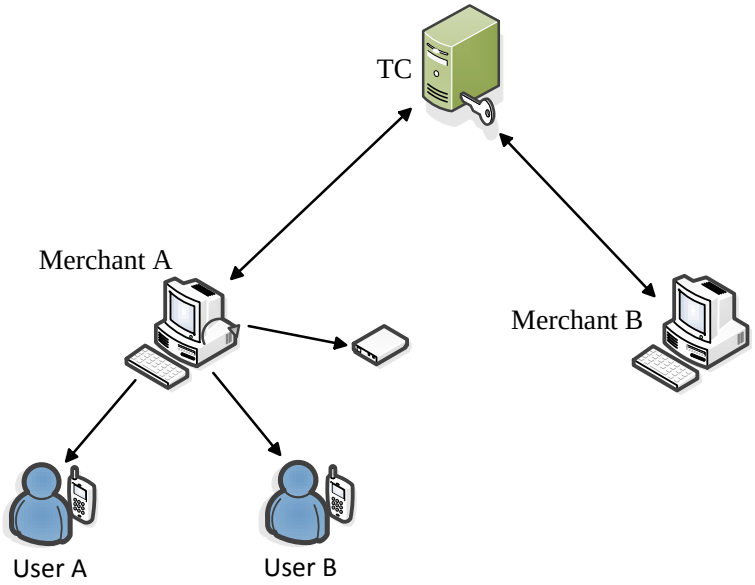


Figure 1: Trusted two-dimensional code system architecture

3.2 Dynamic behavior module

3.2.1 Certificate request module

Certificate application is based on merchant's needs, who applies and obtains the CBS certificate from TC. The behavior module is shown in Figure 2.

(1) TC initializes and generates the system parameters and its public/private key pair; (2) Merchant runs the public key generation module to generate a public key from its private key; (3) Merchant stores the public/private key pair in the database; (4) Merchant launches the CBS certificate request to TC, which contains merchant's public key and identity information; (5) TC authenticates the identity of merchant, and then generates CBS certificate for merchant; (6) TC sends the CBS certificate to merchant either online or offline. Merchant then makes sure if the certificate received successfully.

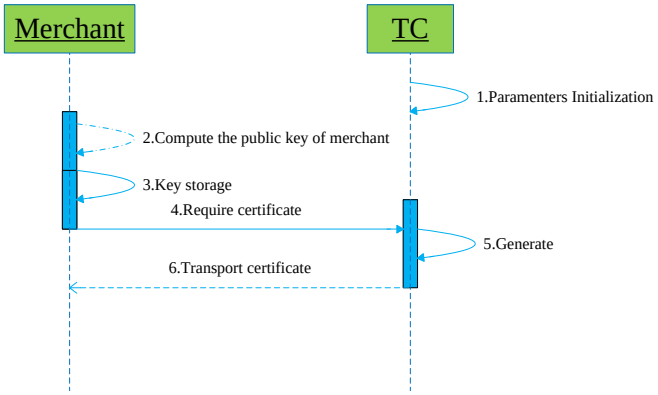


Figure 2: Workflow of certificate application

3.2.2 Signing key generation module

Signing key generation is based on merchant's identity and certificate issued from TC. The behavior module is shown in Figure 3.

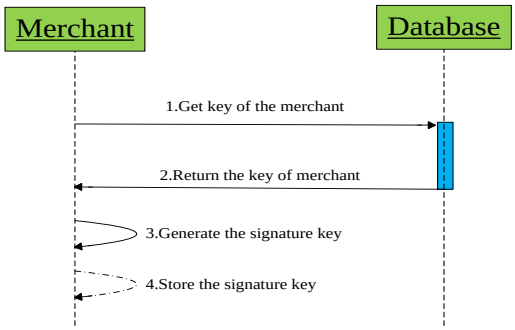


Figure 3: Workflow of signing key generation

(1) Merchant gets the public/private key pair from the database; (2) The database returns the results; (3) Merchant takes its CBS certificate, identity and the public/private key pair as inputs to generate the CBS signing key; (4) The CBS signing key is stored in USBKey for safekeeping.

3.2.3 Two-dimensional code generation module

Two-dimensional code generation is the process for merchant singing the message (m) by the CBS signing key, and coding the results to generate two-dimensional code. The behavior module is shown in Figure 4.

(1) Merchant extracts the signing key from the USBKey; (2) Merchant gets public/private key pair from the database; (3) Database returns the results; (4) Merchant prepares the message which needed to be signed (such as the merchant website etc.); (5) Merchant signs the message by the CBS signing key and generates the corresponding two-dimensional code.

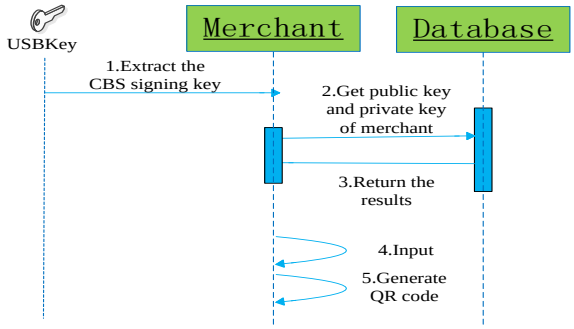


Figure 4: Workflow of two-dimensional code generation

3.2.4 The two-dimensional code verification module

Two-dimensional code verification is the process that user (the consumer who holds the intelligent terminal) scans the two-dimensional code and verifies the signature within the code. The behavioral module is shown in Figure 5.

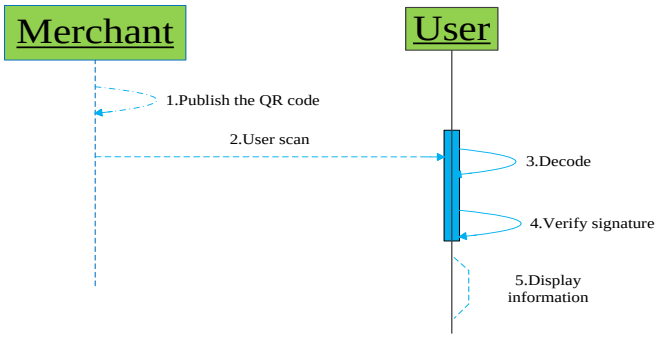


Figure 5: Workflow of two-dimensional code verification process

(1) Merchant released two-dimensional code which previously generated for users to scan; (2) User scans the two-dimensional code by his/her intelligent terminal which installed with the trusted dimensional code software; (3) User decodes the content in the two-dimensional code through Base64; (4) User parses out the signature of the message and verifies the signature to check if it is legitimate; (5) If the validation is successful, user displays the useful message from merchant.

4 System implementation

4.1 System design

As shown in Figure 6, the trusted two-dimensional code system consists of three main parts: TC, two-dimensional code generation, as well as two-dimensional code verification. The system includes eight modules: TC module, certificate application module, certificate generation module, signing key generation module, signing key storage module, two-dimensional code generation module, two-dimensional code scanning module and two-dimensional code verification module.

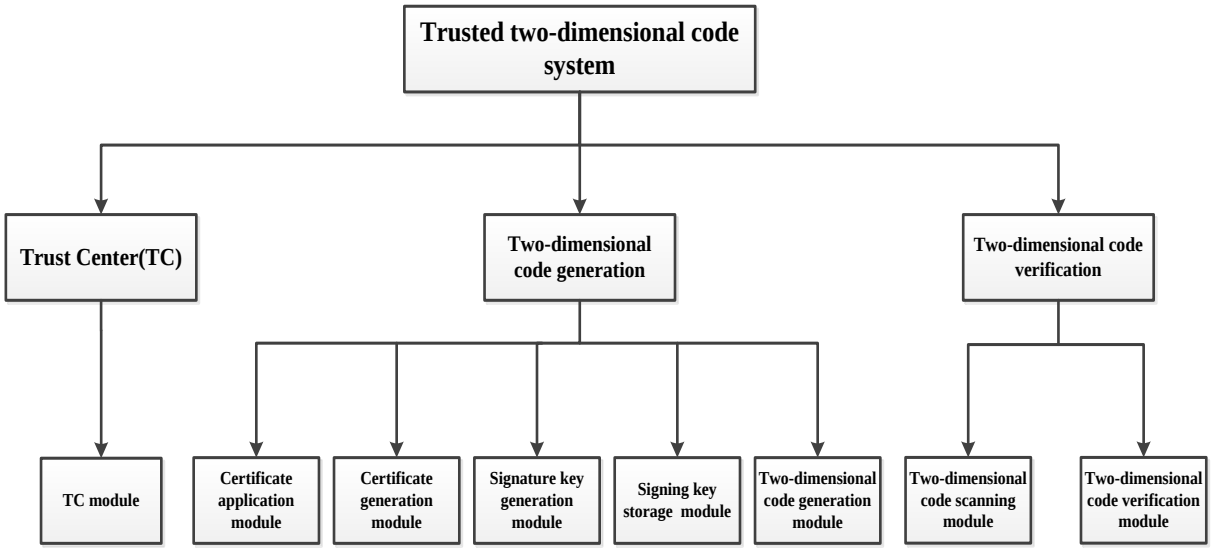


Figure 6: The design of trusted two-dimensional code system

- TC module: This module is mainly responsible for generating system's public parameters and the public/private key pairs of TC and merchant. It is also in charge of the registration form merchant.
- Certificate application module: This module is responsible for sending the merchant's public key and identity information to TC for the legitimacy check.
- Certificate generation module: The module generates and issues the CBS certificate to merchant.
- Signing key generation module: This module obtains merchant's certificate and public/private key pair to generate the signing key.
- Signing key storage module: This module is mainly responsible for storing the signing key into the USBKey to avoid adversary's attack.
- Two-dimensional code generation module: This module encodes the merchant's information together with the signature to generate a two-dimensional code for releasing.
- Two-dimensional code scanning module: The module scans the two-dimensional code and decodes the content in it based on the development interface provided by Zxing library (Google)[8].
- Two-dimensional code verification module: This module is mainly responsible for verifying the signature of the information from merchant.

4.2 Implementation of the key modules

4.2.1 TC, certificate application and generation module

The procedures of system parameters initialization, certificate application acceptance, and certificate generation are shown in Figure 7

Merchant's login interface is shown in Figure 8. The merchant needs to proceed the registration at the first-time login. The necessary information are needed such as account and password. Already registered merchant simply enter the correct user name and password to login.

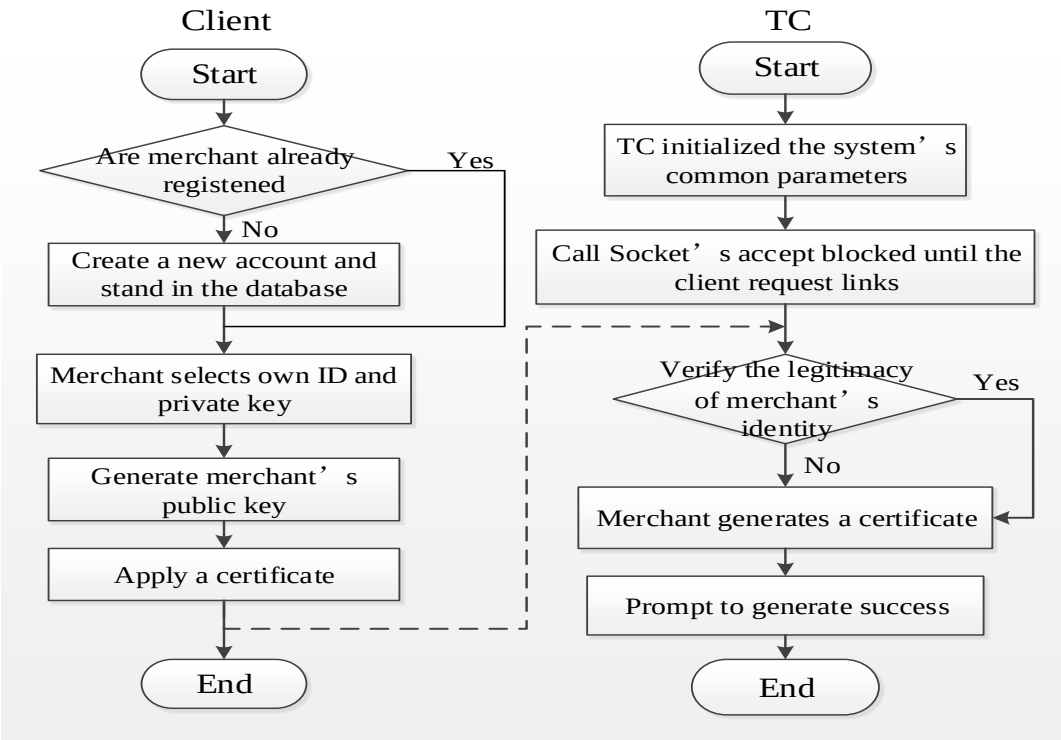


Figure 7: Flow chart of the key module

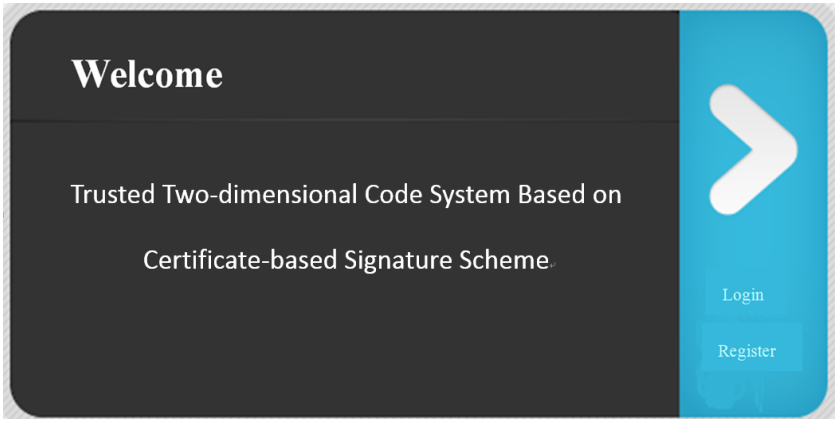


Figure 8: Merchant login interface

4.2.2 Signing key generation module

Signing key generation is a key part of our system. The implementation flow chart is shown in Figure 9.

The result of signing key generation interface is shown in Figure 10. As can be seen from the figure, the premise of the signing key generation is obtaining the CBS certificate from TC.

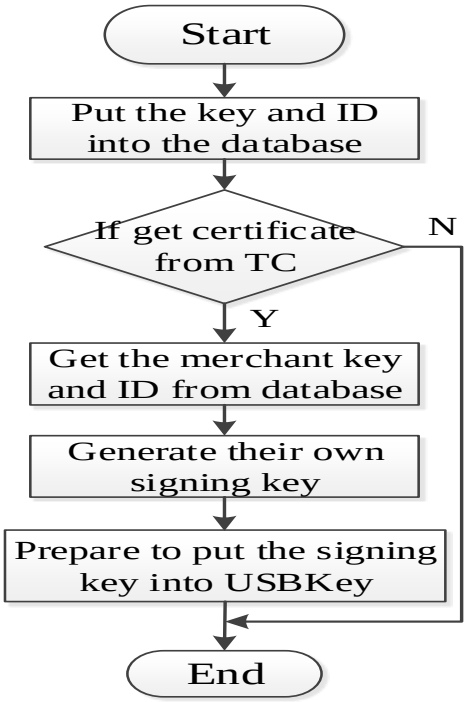


Figure 9: Flow char of signing key generation

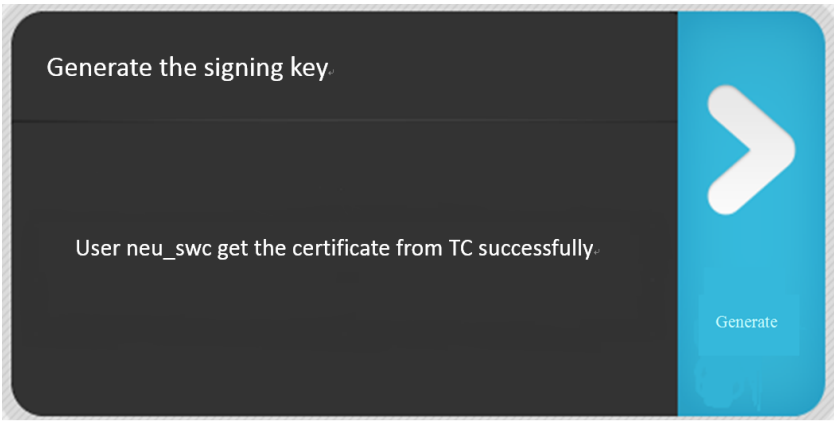


Figure 10: Signing key generation interface

5 Conclusion

The credibility of two-dimensional code is the key point of whether it could be widely used. This paper analyzes the flaws of the two-dimensional code. The TC-based architecture is built for both merchants and users. A trusted two-dimensional code system is then designed and implemented based on CBS signature mechanism, which includes TC part, trusted two-dimensional code generation part, as well as trusted two-dimensional code verification part.

The system is still at its prototype stage. The further implementation and optimization work will be our future research tasks.

Acknowledgement

This work was supported by Major National Scientific & Technological Projects of China under Grant No.2013ZX03002006.

References

[1] Tianhan Gao, Nan Guo, and Kangbin Yim. A hybrid approach to secure hierarchical mobile ipv6 networks. *Computer Science and Information Systems/ComSIS*, 10(2):913–938, 2013.

[2] Craig Gentry. Certificate-based encryption and the certificate revocation problem. In *Advances in Cryptology—EUROCRYPT 2003*, pages 272–293. Springer, 2003.

[3] HuangYU. Two-dimensional code uesd in mobile e-commerce. *Chinese New Communications*, (5):78–80, 2006.

[4] Bo Gyeong Kang, Je Hong Park, and Sang Geun Hahn. A certificate-based signature scheme[c]. In *Topics in Cryptology–CT-RSA 2004*, pages 99–111. Springer, 2004.

[5] Qingbo Kang, Ke Li, and Jichun Yang. A digital watermarking approach based on DCT domain combining QR code and chaotic theory. In *Proc. of the 11th International Conference on Wireless and Optical Communications Networks (WOCN'14), Andhra Pradesh, India*, pages 1–7. IEEE, 2014.

[6] Jiguo Li, Xinyi Huang, Yi Mu, Willy Susilo, and Qianhong Wu. Certificate-based signature: security model and efficient construction. In *Public Key Infrastructure*, pages 110–125. Springer, 2007.

[7] Cátia Santos-Pereira, Alexandre B Augusto, Manuel E Correia, Ana Ferreira, and Ricardo Cruz-Correia. A mobile based authorization mechanism for patient managed role based access control. In *Information Technology in Bio-and Medical Informatics*, pages 54–68. Springer, 2012.

[8] Mabel Vazquez-Briseno, Juan-Ivan Nieto-Hipolito, and Elitania Jimenez-Garcia. Using QR codes to improve mobile wellness applications. *International Journal of computer Science and Network Security*, 10(12):50–54, 2010.

[9] Yu Xiaoyang, Song Yang, Yu Yang, Yu Shuchun, Cheng Hao, and Guan Yanxia. An encryption method for QR code image based on ECA. *International Journal of Security & Its Applications*, 7(5):397–406, October 2013.

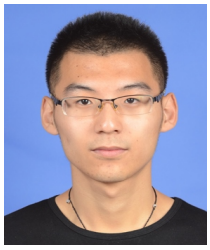
Author Biography

Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained an early promotion to an associate professor in January 2010. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He is the author or co-author of more than 30 research publications. His primary research interests are next generation network security, MIPv6/HMIPv6 security, wireless mesh network security, Internet security, as well as security and privacy in ubiquitous computing.

Luoyin Feng joined Northeastern University in August 20012 as a student of Software College.He obtained the third prize of National Undergraduate Eletronic Design Contest in August 2014.He won the second prize of National College Mathematical Contest in Modeling. His primary research interests are mobile computing and network security.

Yingnan Zhao is an undergraduate student majoring in information security from Northeastern University, China. He has finished the courses like data structures, computer network and cryptography etc. Now, he is participating in the project about trusted two-dimensional code and network security.

Shiyue Qin is an undergraduate student majoring in Information Security at Northeastern University in China. Her primary research interests are identity authentication and mobile computing.



Quanqi Wang as a graduate majors in Information Security at Northeastern University in china.His primary research interest is routing security in WMN.