Privacy Protection Method Based on Two-Factor Authentication Protocol in FRID Systems

Guangquan Xu, Yuanyuan Ren, Nonmembers, Yuanbin Han, Member, Xiaohong Li, Nonmembers, Zhiyong Feng

SUMMARY With the rapid development of Internet of things (IoT), Radio Frequency Identification (RFID) has become one of the most significant information technologies in the 21st century. However, more and more privacy threats and security flaws have been emerging in various vital RFID systems. Traditional RFID systems only focus attention on foundational implementation, which lacks privacy protection and effective identity authentication. To solve the privacy protection problem this paper proposes a privacy protection method with a Privacy Enhancement Model for RFID (PEM4RFID). PEM4RFID utilizes a “2+2” identity authentication mechanism, which includes a Two-Factor Authentication Protocol (TFAP) based on “two-way authentication”. Our TFAP employs “hardware information + AES-ECC encryption”, while the “two-way authentication” is based on improved Combined Public Key (CPK). Case study shows that our proposed PEM4RFID has characteristics of unrepeatability and non-repeatability of instructions, which realizes a good trade-off between privacy and security in RFID systems.

1. Introduction

Radio Frequency Identification (RFID) is one of the most important technologies in the 21st century, which is a perfect combination of wireless communication technology and automatic identification technology [1], [2]. RFID can not only achieve non-contact and rapid multi-target recognition, but the recognition effect is almost uninfluenced by many kinds of bad environment. RFID is widely used in all kinds of public systems which are closely related to privacy, such as the second generation ID card of residents, IC card, Railway Tickets, Magnetic card entrance guard system and so on.

With the wider application of RFID technology in various vital systems, more and more privacy threats and security flaws have been emerging. The attacker can identify some security flaws and invade into RFID systems to steal the user’s data and sensitive information, which seriously violates the privacy of users and damages the credibility of system provider.

A lot of technologies for RFID security and privacy have been put forward by the researchers at home and abroad, which mainly divided into two broad categories: physical methods and identity authentication technology based on cryptography system.

As the name implies, physical methods use physical means to stop the information transfer and protect the privacy of RFID systems. These methods mainly include Kill Tag, Active Interference, Faraday Cage and Block Tag [3], whose application would be limited by the cost and the types of tags.

Identity authentication technology based on cryptographic system uses the transmission of information to achieve the authentication between Tag, Reader and Backend processing system. With the rapid development of the cryptographic techniques, several of cipher algorithms already can achieve hardware implementation. According to the complexity of the cipher algorithm, the identity authentication technology could be divided into three categories [4]: mature authentication technology adopts sophisticated encryption algorithm such as elliptic curve cryptography (ECC), data encryption standard (DES) and advanced encryption standard (AES) and asymmetric encryption cryptography, etc.; Lightweight information authentication technology adopts the HASH function, redundancy check code, random number generator (RNG) and so on, whose calculation amount is relatively small; Ultralightweight information authentication technology adopts equipotential operation of AND, NOT and exclusive or (XOR) for interactive data encryption.

Only in certain conditions, can these techniques achieve data security and privacy protection of RFID systems. That is to say, they almost need improvement.

In order to strengthen identity authentication security and guarantee user’s privacy, this paper proposes a Privacy Enhancement Model for RFID Systems (PEM4RFID) based on “2+2” authentication mechanism, which includes Two-Factor Authentication Protocol (TFAP) and “two-way authentication”.

In this paper, we first investigate RFID technology and its security problems, and put forward Two-Factor Authentication Protocol (TFAP) based on the “hardware device information + AES-ECC encryption”. TFAP could effectively prove user identity legitimacy and avoid the defects of single factor authentication. Next, we introduce the
Combined Public Key (CPK) mechanism into RFID systems and put forward the "two-way authentication" on the basis of the original CPK authentication, which effectively prevents RFID systems from the Denial of Service (DoS) attacks, identity spoofing attacks, and so on. Theoretical analysis shows that "two-way authentication" could achieve the purpose of privacy guarantees and data security. Finally, we propose PEM4RFID based on improved CPK and TFAP. Experimental results show that PEM4RFID successfully strengthens the authentication and privacy guarantees.

The remainder of this paper is organized as follows: Sect. 2 reviews the fundamentals of CPK, Sect. 3 advances the PEM4RFID after introducing TFAP and "two-way authentication", Sect. 4 presents experiments to verify the security performance for our proposed PEM4RFID model, and Sect. 5 summarizes the results and points out the directions for future work.

2. Related Work

2.1 Literature Review

In 1976, Diffie and Hellman [5] published “New Directions in Cryptography” and put forward the public key cryptosystem for the first time, which laid the foundation of public key Cryptography. The algorithm based on mathematical principle separates the encryption key and decryption key. It is extremely difficult to derive the decryption key from the encryption key.

In 1978, Rivest et al [6] put forward RSA cipher system, whose security was based on large integer factorization problem. With the development of computer hardware and High-performance computing (HPC) technology, RSA is no longer safe. RSA not only need more bandwidth, but its encryption efficiency declines.

In this condition, Miller and Koblitz [7], [8] put forward Elliptic Curve Cryptography in 1985, whose security was based on the elliptic curve discrete logarithm problem (ECDLP). ECC requires less network bandwidth, but has strong ability against attack [9]. ECC transplanted the traditional encryption algorithm to the elliptic curve, which achieves key exchange protocol, data encryption and digital signature. In 1996, Public Key Infrastructure (PKI) began to form, greatly promoted the creation and development of authentication theory. PKI proposed the concept of third party certification for the first time. PKI uses hierarchical Certificate Authority (CA) authentication centers to release digital certificates, verify the user’s identity information and prove its credibility. As PKI expanding the scale of the key management, it requires a great deal of network traffic [10] but has small capacity.

On the basis of PKI, Identity Based Encryption (IBE) was proposed. In 1984, Shamir successfully proves the existence of the key algorithm based on identification. In 2001, IBE algorithm was proposed by Don Boneh and Matthew Franklin [11]. IBE adopts a new private key distribution scheme, undo the CA authentication center, retained the user preferences, and just need online parameter library support. But IBE couldn’t adapt to the actual application environment.

In 2006, Nan [12] proposed a more credible certification mechanism: CPK authentication system.

2.2 Basic Knowledge of CPK

CPK is based on Elliptic Curve [13]. Elliptic curve is a curve defined in a variety of limited domains. That is to say, CPK depends on the elliptic curve group $E_p(a, b)$ based on prime integer fields [14] (e.g., see Eq. (1)).

$$y^2 \equiv (x^3 + ax + b) \mod p$$

with curve parameters $a, b, p \in GF(p)$. Pick up a basis point $G$ from $E_p(a, b)$.

$$G = (x, y)$$

If $P = (x_1, y_1), Q = (x_2, y_2), P \neq \pm Q$, addition rules of elliptic curve are shown in Eq. (3)–(5).

$$P + Q = (x_3, y_3)$$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

Multiplication rules of elliptic curve are shown in Eq. (6)–(8).

$$2P = (x_4, y_4)$$

$$x_4 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

$$y_4 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

In terms of addition and multiplication rules of elliptic curve, a multiple point set, namely generated subgroup $S_G$, can be calculated based on point $G$.

$$S_G = \{G, 2G, 3G, \ldots, nG\}$$

Pick up multiple point $kG$ from $S_G$, and $k$ is the discrete logarithm of multiple point $K$.

$$kG = K = (x_k, y_k)$$

Mathematic research shows that $K$ is calculated easily with $k$ and $G$ known [15]. But it is almost impossible to get $k$ with $K$ and $G$ known. This is a classic elliptic curve discrete logarithm problem, which is the origin of ECC.

3. Privacy Enhancement Model

In this paper, we proposed a RFID privacy enhancement
model PEM4RFID. In order to protect the privacy of users, PEM4RFID adopts the Two-Factor Authentication Protocol (TFAP) based on the “hardware device information + AES-ECC encryption”. In addition, TFAP adopts the two-way authentication based on improved CPK to authenticate the identity between Tag, Reader and Backend processing system. Thus, TFAP can effectively prevent the RFID systems from the DoS attacks, identity spoofing attacks, and so on, achieve the purpose of user privacy guarantees and data security. The model structure of PEM4RFID is shown in Fig. 1.

3.1 Two-Factor Authentication Protocol

There are many traditional authentication methods, but they simply adopt one of the single factor authentication principles. First, traditional authentication methods usually authenticate the identity of users according to user’s information such as the static password. Secondly, these methods use objects users holding to authenticate the identity such as smart card, seal, and so on. Finally, these methods can also make use of unique physical characteristics of user to authenticate the identity such as fingerprint, iris, DNA and other biological characteristics. Because these methods are based on single factor authentication, there will be more or less potential security risks such as seal stolen, static password lost, and so on. These risks will lead to serious damage of user privacy.

In order to solve the potential safety risk, we put forward TFAP, a two-factor authentication protocol of RFID systems. TFAP is based on the “hardware device information + AES-ECC encryption”. “Hardware information” means fixed configuration information in CPK chips. A reader or a backend processing system will be configured a chip with unique identification sequence code and key matrix. “AES-ECC encryption” means the encryption system combined AES with ECC. In this paper, the AES algorithm is used to encrypt plaintext, ECC algorithm is used to encrypt AES key.

With the combination of “Hardware information” and “AES-ECC encryption”, TFAP adopts the chip technology and the encryption technology to implement the functions of RFID systems, such as identity authentication, data encryption, data decryption, and so on. The private keys are only generated in the CPK chips and closely guarded at the hardware level. The private keys are only allowed to be used within the CPK chips. In other words, the private keys will play no part outside the CPK chips. When an attacker attempts to dissect chip and obtain chip data illegally, the chip data will be automatically destroyed. So, the attacker can never get a complete private key [16], [17]. Even if the attacker intercepts the signal of RFID systems illegally, the attacker is still unable to get any information for AES-ECC encryption based on discrete logarithm problem.

Our TFAP protocol algorithm is described as follows.

### 3.1.1 System Initialization

According to the elliptic curve group $E_p(a, b)$, the secret key management center builds the private key matrix $skm$ and public key matrix $PKM$.

$$skm = \begin{pmatrix} s_{1,1} & \ldots & s_{1,32} \\ \vdots & \ddots & \vdots \\ s_{32,1} & \ldots & s_{32,32} \end{pmatrix}_{32 \times 32}$$  \hspace{1cm} (11)

$$PKM = \begin{pmatrix} (a_{1,1}, b_{1,1}) & \ldots & (a_{1,32}, b_{1,32}) \\ \vdots & \ddots & \vdots \\ (a_{32,1}, b_{32,1}) & \ldots & (a_{32,32}, b_{32,32}) \end{pmatrix}_{32 \times 32}$$  \hspace{1cm} (12)

Pick up a basis point $G$ from $p(a, b)$.

$$G = (x_0, y_0)$$  \hspace{1cm} (13)

### 3.1.2 User A Sends the Digital Signature to User B

User A selects a random number $p$, computes digital signature code with unique identification sequence code of CPK chip.

The algorithm is described by pseudocode as follows.

a) Random $r = \text{new Random}()$

\[ p = r.\text{nextInt}((\text{sec}.\text{getN}())) \]

b) $(x_p, y_p) = p * \text{ee}.\text{getG}()$

c) $c = (x_p + y_p)^2 \mod 2^m$

d) $s = p^{-1}(h + c * a) \mod n$

e) $sign = (s, c)$

### 3.1.3 User B Verifies the Digital Signature of User A

User B receives signals of User A, verifies the digital signature code.

a) $s = \text{sign}.\text{getS}()$

\[ c = \text{sign}.\text{getC}() \]

b) $(x'_p, y'_p) = s^{-1}hG + s^{-1}cA$

c) $c' = (x'_p + y'_p)^2 \mod 2^m$

d) If $c = c'$ then return true

else return false

### 3.1.4 User B Sends the Digital Signature to User A

User B selects a random number $q$, computes digital signature code with unique identification sequence code of CPK.
3.1.5 User A Verifies the Digital Signature of User B

User A receives signals of User B, verifies the digital signature code.

a) \( s = sign\).get\(S() \)
   \( c = sign\).get\(C() \)

b) \( (x'_q, y'_q) = s^{-1}hG + s^{-1}cB \)

c) \( c' = (x'_q + y'_q)^2 \mod 2^m \)

d) if \( c = c' \) then return true
   else return false

After this, the two-way authentication between User A and User B is completed, they can communicate with each other.

3.1.6 User B Encrypts Data

Based on AES-ECC encryption, User B chooses a random number and calculates the value of \( key \).

a) \( \beta = ENC\_A(key) \)
b) \( code = E_{key}(data) \)
c) \( Send\_To\_A = \{code, \beta\} \)

3.1.7 User A Decrpyts Data

a) \( Receive\_From\_B = \{code, \beta\} \)
b) \( key = DEC\_A(\beta) \)
c) \( data = D_{key}(code) \)

3.1.8 User A Extracts and Stores Data

User A extracts the decrypted data and then stores the data.

All in all, TFAP guarantees the legitimacy of the user’s identity, so the attacker is ultimately difficult to decrypt the signal of RFID systems.

3.2 Two-Way Authentication Based on Improved CPK

CPK authentication is one-way. So, when User A plans to send message to User B, it is only required that User A sends digital signature to User B and User B verifies it [18], [19]. But TFAP proposed in this paper, adopts the two-way authentication to authenticate the identity between Tag, Reader and Backend processing system. Only when both sides authenticate each other successfully, can the data or instructions be encrypted and send.

3.3 Model Design of PEM4RFID

CPK authentication system is a kind of mature identity authentication system. AES-ECC encryption adopts complex encryption algorithm. As a result of that, PEM4RFID makes use of active tags whose computing power is especially strong. PEM4RFID not only can provide efficient safety protection with TFAP, but also follows the two-way authentication to enhance the privacy of users. The working principle of PEM4RFID is shown in Fig. 3.

Working principles between tags and reader are followed.

1. The control program of reader selects a random number \( k \), computes digital signature code with unique identification sequence code of CPK chip, and sends signature code via radio frequency interface.
2. The tag receives signals of reader, verifies the digital signature code. If the verification is successful, go to step (3); else the tag will discard the signal, clear the buffer zone, and refuse to receive the signals of same reader.
3. The control program of tag selects a random number \( k \), computes digital signature code with unique identification sequence code of tag chip, and sends signature code via tag antenna.
4. The reader receives signals of tag, verifies the digital signature code. If the verification is successful, the reader is ready to receive signals of same tag. If the verification is failing, the reader will discard the signal, clear the buffer zone, and refused to receive the signals of same tag.
5. Based on AES-ECC encryption, the tag chooses a random number and calculates the value of \( key \). Then, the tag calculates \( ENC\_READER(\text{key}) = \beta \), \( E_{\text{key}}(\text{data}) = code \), and sends \( \{code, \beta\} \) to reader.
6. The reader receives \( \{code, \beta\} \) and calculates
The working principle of PEM4RFID.

\[ \text{DEC}_{\text{reader}}(\beta) = \text{key}, \text{D}_{\text{key}}(\text{code}) = \text{data}. \]

(7) The reader extracts and stored data.

Working principles between the reader and the backend processing system are followed.

1. The control program of reader selects a random number \( k \), computes digital signature code with unique identification sequence code of CPK chip, and sends signature code to backend processing system via cable channel or wireless channel.
2. The backend system receives signals of reader, verifies the digital signature code. If the verification is successful, go to step (3); else the backend system will discard the signal, clear the buffer zone, and refuse to receive the signals of same reader.
3. The backend system selects a random number \( k \), computes digital signature code with unique identification sequence code of CPK chip, and sends signature code via cable channel or wireless channel.
4. The reader receives signals of backend system, verifies the digital signature code. If the verification is successful, the reader is ready to receive signals of same backend system. If the verification is failing, the reader will discard the signal, clear the buffer zone, and refused to receive the signals of same backend system.
5. Based on AES-ECC encryption, the backend system chooses a random number and calculates the value of key. Then, the backend system calculates \( \text{ENC}_{\text{reader}}(\text{key}) = \beta, \text{E}_{\text{key}}(\text{Instruction}) = \text{code} \), and sends \( \text{code}, \beta \) to reader.
6. The reader receives \( \text{code}, \beta \) and calculates \( \text{DEC}_{\text{reader}}(\beta) = \text{key}, \text{D}_{\text{key}}(\text{code}) = \text{Instruction} \).
7. The reader extracts and performs the Instruction.

In cryptography, \( \text{ENC} \) is asymmetric encryption function, and especially means ECC encryption function in this paper. \( E \) is symmetric encryption function, and especially means AES encryption function.

\( \text{DEC} \) is asymmetric decryption function, and especially means ECC decryption function in this paper. \( D \) is symmetric decryption function, and especially means AES decryption function.

\( \text{READER} \) is the public key of reader and \( \text{reader} \) is the private key.

4. Case Study

4.1 Why Choose AES and ECC

In this paper, the AES algorithm is used to encrypt plaintext, ECC algorithm is used to encrypt AES key. AES is symmetrical encryption algorithm. Its encryption speed is especially fast, AES is suit for encrypting long plaintext. However, the shortcoming is the key management of AES is complex and unsafe.

ECC is asymmetrical encryption algorithm, which is easy for key management. Therefore, ECC is very suitable for key encryption and digital signature.

AES-ECC encryption synthesizes the advantages of symmetric encryption and asymmetrical encryption, which solves the problem of efficiency and safety in the communication. Although the mixed AES-ECC encryption is divided into two stages, the efficiency is higher than ever before.

4.2 Example

According to the elliptic curve group \( E_{541}(116, 11) \), we utilize an example, a communication between reader and tag, to verify the feasibility of PEM4RFID. The sequence diagram is shown in Fig. 4.

Usually, owe-way authentication can resist a guess attack but suffer from replay and man-in-the-middle attacks. As a verifier, the tag simply controls its data while the reader to be authenticated is likely to be cheated. However, our proposed PEM4RFID can effectively prevent these potential safety risks happening based on two-way authentication.

Moreover, traditional One-Factor Authentication fails to provide strong authentication as a consequence of the unreliability of single factor such as password stolen. However, our proposed PEM4RFID has feasibility to avoid such problems based on Two-Factor Authentication Protocol.

PEM4RFID utilizes a “2+2” identity authentication mechanism to efficiently enhance the security of system, which includes a Two-Factor Authentication Protocol (TFAP) based on “two-way authentication”.

4.2.1 System Initialization

According to the elliptic curve group \( E_{541}(116, 11) \), the secret key management center builds the private key matrix \( \text{skm} \) and public key matrix \( \text{PKM} \).
reader and the tag can communicate with each other.

The control program selects a random number \( p = 2 \), computes digital signature code with unique identification sequence code of CPK chip.

\[
\text{PKM} = \begin{pmatrix}
(10,508) & \ldots & (506,35) \\
\vdots & \ddots & \vdots \\
(300,204) & \ldots & (55,415)
\end{pmatrix}_{32 \times 32}
\]

Pick up a basis point \( G \) from \( E_{541} (116, 11) \).

\[
G = (257, 290)
\]

4.2.2 Digital Signature of Reader

The tag receives signals of reader, verifies the digital signature code.

\[
\text{skm} = \begin{pmatrix}
13 & \ldots & 16 \\
\vdots & \ddots & \vdots \\
35 & \ldots & 26
\end{pmatrix}_{32 \times 32}
\]

\[
\text{sign} = (s, c) \xleftarrow{} (26, 9) \text{ via radio frequency interface}
\]

4.2.3 Tag Verifies the Digital Signature of Reader

The tag verifies the digital signature code of reader, verifies the digital signature code.

\[
\text{skm} = \begin{pmatrix}
13 & \ldots & 16 \\
\vdots & \ddots & \vdots \\
35 & \ldots & 26
\end{pmatrix}_{32 \times 32}
\]

4.2.4 Digital Signature of Tag

The control program of tag selects a random number \( q, q = 3 \), computes digital signature code with unique identification sequence code of tag chip.

\[
\text{PKM} = \begin{pmatrix}
(10,508) & \ldots & (506,35) \\
\vdots & \ddots & \vdots \\
(300,204) & \ldots & (55,415)
\end{pmatrix}_{32 \times 32}
\]

4.2.5 Reader Verifies the Digital Signature of Tag

The reader receives signals of tag, verifies the digital signature code.

\[
\text{skm} = \begin{pmatrix}
13 & \ldots & 16 \\
\vdots & \ddots & \vdots \\
35 & \ldots & 26
\end{pmatrix}_{32 \times 32}
\]

4.2.6 Tag Encrypts Data

Based on AES-ECC encryption, the tag chooses a random number and calculates the value of \( \text{key}=13924 \). data='hello'.

\[
a) \text{Compute } \beta = \text{ENC}_{\text{READER}}(\text{key}) = (337, 521) \\
b) \text{Compute } \text{code} = \text{E}_{\text{key}}(\text{data}) \\
c) \text{Send } \{\text{code}, \beta\} \text{ to reader}
\]

4.2.7 Reader Decrypts Data

\[
a) \text{The reader receives } \{\text{code}, \beta\} \\
b) \text{Compute } \text{key} = \text{DEC}_{\text{READER}}(\beta) = 13924 \\
c) \text{data} = D_{\text{key}}(\text{code}) = \text{hello}
\]

4.2.8 The Reader Extracts and Stores Data

The reader extracts the decrypted data and then stores the data.

4.3 Security Performance Analysis

PEM4RFID adopts the two-way authentication based on improved CPK, which is effective for authentication. If the verification is failing, PEM4RFID will discard the signal, clear the buffer zone, and refused to receive the signals of same origin. There will be buffer overflow in RFID systems. Therefore, this model can effectively prevent direct attack such as DoS attacks.

PEM4RFID adopts the chip technology. The private keys are only generated in the CPK chips and closely guarded at the hardware level. The private keys are only allowed to be used within the CPK chips. In other words, the private keys will play no part outside the CPK chips. When an attacker attempts to dissect chip and obtain chip data illegally, the chip data will be automatically destroyed. So, the attacker can never get a complete private key.

PEM4RFID adopts AES-ECC encryption technology. It is almost impossible to get private key with public key known. This is the classic elliptic curve discrete logarithm problem[20], [21]. Even if the attacker intercepts the signals of RFID systems illegally, the attacker is still unable to get any information from the signals.

PEM4RFID is based on TFAP. Only when verifying signature successfully, can PEM4RFID send encrypted data or instructions. The attacker can neither distinguish different tags nor record the route by eavesdropping communication signals. Therefore, PEM4RFID can effectively prevent RFID systems from identity spoofing attacks or tag tracking attacks.

In addition, PEM4RFID will choose a random number for realtime digital signature and data encryption. So, even sending the same data, PEM4RFID will calculate the
different signature or cipher at different time. Therefore, PEM4RFID have nonrepeatability of instructions, which effectively prevent replay attacks or spoofing attacks. The attacker cannot illegally obtain the privacy data of user.

To sum up, PEM4RFID can supply a good trade-off between privacy and data security.

5. Conclusion and Future Work

In this paper, we propose a novel identity authentication mechanism based on “2+2” authentication mechanism. First, we put forward two-factor authentication protocol TFAP based on the “hardware device information + AES-ECC encryption”. TFAP could effectively prove user’s identity legitimacy and avoid the defects of single factor authentication. Next, we introduce the improved CPK into RFID systems and put forward the “two-way authentication”, which effectively prevents the RFID systems from the DoS attacks, identity spoofing attacks, and so on. Theoretical analysis shows that “two-way authentication” could achieve a good trade-off between privacy protection and data security.

In this paper, we adopt active tags in RFID systems. However, mobility of active tags is poor and the cost is higher than passive tags. So our future work is to improve the PEM4RFID model to make use of passive tags.

Acknowledgments

This work is supported by the National Natural Science Foundation of China(No. 61340039, 61572355, 61572349), Foundation of Hebei Educational Committee (No.YQ2014014) and 985 funds of Tianjin University, Tianjin Research Program of Application Foundation and Advanced Technology under grant No. 15JCYBJC15700 and No. 14JCTPJC00517.

References


Guangquan Xu is a Ph.D. and associate professor in the School of Computer Science and Technology, Tianjin University, China. He received Ph.D. degree from Tianjin University in March 2008. He is a member of the CCF and ACM. His research interests include trusted computing, trust and reputation, cyber security, middleware.

Yuanyuan Ren is a master student in the School of Computer Science and Technology, Tianjin University, China. She receives the B.S. degree in School of Software, Tianjin Normal University in 2015. Her current research is about identity authentication.

Yuanbin Han is a lecturer in School of Information and Electrical Engineering, Hebei University of Engineering, Handan, Hebei, China. He received the Ph.D. degrees in School of Computer Science and Technology, Tianjin University, China.
Xiaohong Li is a full tenured professor of the School of Computer Science and Technology, Tianjin University, Tianjin, China. Her current research interests include knowledge engineering, trusted computing, and security software engineering.

Zhiyong Feng is a full tenured professor and head of the School of Computer Science and Technology, Tianjin University, Tianjin, China. His current research interests include knowledge engineering, service computing, and security software engineering.