International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.345-354
http://dx.doi.org/10.14257/ijsia.2013.7.6.35

Study of the Privacy Models in RFID Authentication Protocols

Jian Shen[*1,2], Wenying Zheng[3], Jin Wang[1,2], Zhihua Xia[1,2] and Zhangjie Fu[1,2]

[1]*Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science &Technology, Nanjing, 210044, China*
[2]*School of Computer & Software, Nanjing University of Information Science &Technology, Nanjing, 210044, China*
[3]*School of Applied Meteorology, Nanjing University of Information Science &Technology, Nanjing, 210044, China*

Abstract

Privacy is a major concern in RFID systems, especially with widespread deployment of wireless enabled interconnected personal devices. In this paper, we consider privacy issues in RFID system where the authorized readers must be able to identify tags without an adversary being able to trace them, and provide a formal security model for privacy in RFID system. Under this model, we analyze the recently proposed RFID authentication protocol named anonymous RFID authentication protocol and show attacks on them that compromise the privacy.

Keywords: *privacy model; untraceability; RFID*

1. Introduction

A passive radio-frequency identification (RFID) tag is a microchip that is capable of transmitting a static identifier or serial number for a short distance. It is typically activated by a query from a nearby reader, which also transmits power for the operation of the tag. Nowadays, RFID is used in a wide variety of applications, from the small plaques mounted on car windshields for the purpose of automated toll payment to the theft-detection tags attached in shops to consumer goods, and the proximity cards used to control physical access to buildings.

Privacy is a significant concern that needs to be addressed in terms of tag anonymity and tag untraceability when RFIDs are to be as widely deployed as conceived by proponents. Tag anonymity requires that the tag ID should be kept anonymous in order to solve the problem of leaking information pertaining to the user belongings. Tag untraceability requires that the output of the tag should not be constant in order to avoid adversary tracking. If the output of the tag is fixed, the adversary can easily track the tag. In addition, in the worst case, *i.e.*, secret information in the tag can be obtained by an adversary due to the tag being not the tamper-resistant hard-ware, forward security is required for preventing an adversary from tracking the past events.

In this paper, we focus on providing a security model for solving the above privacy issues and analyzing the recently proposed RFID authentication protocol named anonymous RFID authentication protocol [1] proposed by Shen *et. al.*, in order to show its vulnerability. Until now, a rigorous treatment of privacy for RFID models is still being developed. It is worth

* The corresponding author

ISSN: 1738-9976 IJSIA

noting that some famous models have already been proposed by Avoine [2], Juels and Weis [3], Le Burmester and de Medeiros [4], and Vaudenay [5]. These models differ mainly in their treatment of the adversary's ability to corrupt tags. In this paper, our model is based on Juels-Weis model and allows the adversary to corrupt tags to obtain the secret information.

The rest of this paper is organized as follows: In the following section, some related works are briefly introduced. A security model for privacy is described in detail in Section 3. Security analysis of the anonymous RFID authentication protocol is presented in Section 4. Finally, the conclusions of this paper are covered in Section 5.

2. Related Works

The success of RFID tag implementations depends on addressing privacy and security issues surrounding the use of RFID tags. People always hope that their privacy and security are able to be protected. However, a majority of existing RFID tag implementations are not secure, even though the RFID technology increases the safety of food and drugs through proper monitoring and counterfeit prevention. These tags can broadcast information about their presence so that an adversary can silently track and monitor the presence of an RFID tag from a distance without the knowledge of the person holding the tagged object [6]. Lots of researches focus on designing authentication protocols in RFID-tagged systems to protect the privacy and security of the use of RFID tags. Interested readers can refer to recent survey papers [7] for more details.

Many simple challenge-response protocols have been proposed. The Ohkubo-Suzuki-Kinoshita protocol (OSK) [8] made forward privacy possible. A few attempts have been made to really formalize privacy in RFID protocols. One of the first attempts was made by Avoine [2]. Following their model, privacy is formalized by the ability to distinguish two known tags. Juels and Weis [3] extended this model using side-channel information and making the two target tags chosen by the adversary. Another model was proposed by Burmester and de Medeiros [4]. Our security model is defined based on Juels and Weis model. Recently, Shen et.al proposed an anonymous RFID authentication protocol [1]. However, under the well defined security model below, it is vulnerable to active attacks and violates the privacy requirements.

3. Security Model and Definitions

3.1. Model

Communication between readers and tags is provided via a wireless network, upon which third parties can easily eavesdrop and which is easily cut or disturbed. A protocol party is a $\mathcal{T} \in$ Tags or $\mathcal{R} \in$ Readers interacting in protocol sessions as per the protocol specifications until the end of the session upon which each party outputs **Accept** if it feels the protocol has been normally executed with the correct parties. Adversary $\mathcal{A}$ controls the communications between all protocol parties (tag and reader) by interacting with them as defined by the protocol, formally captured by $\mathcal{A}$'s ability to issue queries of the following form:

Execute($\mathcal{R}$, $\mathcal{T}$, i) query. This models passive attacks, where adversary $\mathcal{A}$ gets access to an honest execution of the protocol session i between $\mathcal{R}$ and $\mathcal{T}$ by eavesdropping.

Send(U_1, U_2, i, m) query. This query models active attacks by allowing the adversary $\mathcal{A}$ to impersonate some reader U_1 in some protocol session i and send a message m of its choice to an instance of some tag U_2. It is worth noting that U_1 can also be tag and U_2 can be reader.

Corrupt($\mathcal{T}$, K) query. This query allows the adversary $\mathcal{A}$ to learn the stored secret K'of the tag $\mathcal{T}$, and which further sets the stored secret to K. It captures the notion of forward security or forward privacy and the extent of the damage caused by the compromise of the tag's stored secret.

Test(U, i) query. This query is the only query that does not correspond to any of $\mathcal{A}$'s abilities or any real-world event. This query allows to define the indistinguishability-based notion of untraceable privacy (**UPriv**). If the party has accepted and is being asked a **Test** query, then depending on a randomly chosen bit $b \in \{0, 1\}$, $\mathcal{A}$ is given $\mathcal{T}_b$ from the set $\{\mathcal{T}_0, \mathcal{T}_1\}$. Informally, $\mathcal{A}$ succeeds if it can guess the bit b. In order for the notion to be meaningful, a **Test** session must be fresh, which means the party has not been sent a **Corrupt** query.

3.2. Privacy Definition

It is worth noting that anonymity can be easily achieved, so we define the untraceability in detail here.

Definition 1 (RFID Untraceable Privacy)

Untraceable privacy (**UPriv**) is defined using the game $\mathcal{G}$ played between a malicious adversary $\mathcal{A}$ and a collection of reader and tag instances. $\mathcal{A}$ runs the game $\mathcal{G}$ whose setting is as follows.

Phase 1 (Learning): $\mathcal{A}$ is able to send any **Execute**, **Send**, and **Corrupt** queries at will.

Phase 2 (Challenge):

1. At some point during $\mathcal{G}$, $\mathcal{A}$ will choose a fresh session on which to be tested and send a **Test** query corresponding to the test session. Note that the test session chosen must be fresh, which means the party has not been sent a **Corrupt** query. Depending on a randomly chosen bit $b \in \{0, 1\}$, $\mathcal{A}$ is given $\mathcal{T}_b$ from the set $\{\mathcal{T}_0, \mathcal{T}_1\}$.

2. $\mathcal{A}$ continues making any **Execute**, **Send**, and **Corrupt** queries at will, subjected to the restrictions that the parties have not been sent **Corrupt** queries.

Phase 3 (Guess): Eventually, $\mathcal{A}$ terminates the game simulation and outputs a bit b', which is its guess of the value of b.

The success of $\mathcal{A}$ in winning $\mathcal{G}$ and thus breaking the notion of **UPriv** is quantified in terms of $\mathcal{A}$'s advantage in distinguishing whether $\mathcal{A}$ received $\mathcal{T}_0$ or $\mathcal{T}_1$. It means that $\mathcal{A}$ correctly guesses the value of b. This is denoted by $Adv_A^{\text{UPriv}}(k)$ where k is the security parameter. We conclude that an RFID authentication protocol with security parameter k is untraceable private if:

$$Adv_A^{\text{UPriv}}(k) = \left| \Pr[A\ win] - \frac{1}{2} \right| = \left| \Pr[b' = b] - \frac{1}{2} \right| \leq 1/\text{poly}(k),$$

where 1/poly(k) denotes a negligible function, which can also be expressed as $\varepsilon(k)$.

Definition 2 (Tag Unforgeability) Our definition of tag unforgeability (***TUF***) for the proposed protocol characterizes the ability of adversary $\mathcal{A}_{\mathrm{TUF}}$ to clone valid-looking tags in an RFID system. ***TUF*** is defined using the game $\mathcal{G}_{\mathrm{TUF}}$ played between a malicious adversary $\mathcal{A}_{\mathrm{TUF}}$ and a collection of reader and tag instances, in which $\mathcal{A}_{\mathrm{TUF}}$ interacts with the reader and with tags for an arbitrary period of time determined by $\mathcal{A}_{\mathrm{TUF}}$. $\mathcal{A}_{\mathrm{TUF}}$ runs the game $\mathcal{G}_{\mathrm{TUF}}$ whose setting is as follows.

Phase 1 (Learning): $\mathcal{A}_{\mathrm{TUF}}$ is able to send any **Execute**, **Send** queries at will.

Phase 2 (Challenge): In the challenge phase, the adversary $\mathcal{A}_{\mathrm{TUF}}$ has no oracle access to tags. $\mathcal{A}_{\mathrm{TUF}}$ outputs a message to query $\mathcal{R}$ until $\mathcal{R}$ yields some output γ.

if $\mathcal{R}$ accept then
  output '1' ;
else
  output '0' ;
Then, $\mathcal{A}_{\mathrm{TUF}}$ terminates the game simulation.

The goal of $\mathcal{A}_{\mathrm{TUF}}$ is to cause $\mathcal{R}$ to accept at least once. The success of $\mathcal{A}_{\mathrm{TUF}}$ in winning $\mathcal{G}_{\mathrm{TUF}}$ and thus breaking the notion of ***TUF*** is quantified in terms of $\mathcal{A}_{\mathrm{TUF}}$'s advantage in causing $\mathcal{R}$ to output "γ = 1". This is denoted by $Adv_{A_{TUF}}^{TUF}(k)$ where k is the security parameter. Hence, our concrete definition of ***TUF*** is given as follows:

A protocol in an RFID system with security parameter k is tag unforgeable if:

$$Adv_{A_{TUF}}^{TUF}(k) = \Pr[A_{TUF}{}^{E,S} \quad win\, G_{TUF}]$$
$$= \Pr[\gamma = 1] \le \varepsilon(k) \quad ,$$

where $\varepsilon(k)$ is negligible function of k[1].

Definition 3 (Reader Unforgeability) Reader unforgeability (***RUF***) is defined using the game $\mathcal{G}_{\mathrm{RUF}}$ played between a malicious adversary $\mathcal{A}_{\mathrm{RUF}}$ and a collection of reader and tag instances, in which $\mathcal{A}_{\mathrm{RUF}}$ interacts with the reader and with tags for an arbitrary period of time determined by $\mathcal{A}_{\mathrm{RUF}}$. $\mathcal{A}_{\mathrm{RUF}}$ runs the game $\mathcal{G}_{\mathrm{RUF}}$ whose setting is as follows.

Phase 1 (Learning): $\mathcal{A}_{\mathrm{RUF}}$ is able to send any **Execute**, **Send** queries at will.

Phase 2 (Challenge): In the challenge phase, the adversary $\mathcal{A}_{\mathrm{RUF}}$ has no oracle access to readers. $\mathcal{A}_{\mathrm{RUF}}$ outputs a message to query $\mathcal{T}$ until $\mathcal{T}$ yields some output η.

if $\mathcal{T}$ accept then
  output '1' ;
else
  output '0' ;

Then, $\mathcal{A}_{\mathrm{RUF}}$ terminates the game simulation.

The goal of $\mathcal{A}_{\mathrm{RUF}}$ is to cause $\mathcal{T}$ to accept at least once. The success of $\mathcal{A}_{\mathrm{RUF}}$ in winning $\mathcal{G}_{\mathrm{RUF}}$ and thus breaking the notion of ***RUF*** is quantified in terms of $\mathcal{A}_{\mathrm{RUF}}$'s advantage in causing $\mathcal{T}$ to output "η = 1". This is denoted by $Adv_{A_{RUF}}^{RUF}(k)$ where k is the security parameter. Hence, our concrete definition of ***RUF*** is given as follows:

[1] A function is negligible if it approaches zero faster than the reciprocal of any polynomial $p(k)$. More formally, $\varepsilon : \square \to \square$ is negligible if for any nonzero polynomial $p(\cdot)$ there exists an m such that $\forall n > m, |\varepsilon(n)| < 1/\, p(n)$.

A protocol in an RFID system with security parameter k is reader unforgeable if:

$$Adv_{A_{RUF}}^{RUF}(k) = \Pr[A_{RUF}{}^{E,S} \quad win\, G_{RUF}]$$
$$= \Pr[\eta = 1] \le \varepsilon(k) \quad ,$$

where $\varepsilon(k)$ is negligible function of k.

Definition 4 (Forward Security) Our definition of forward security (***FS***) for the proposed protocol characterizes the ability of adversary $\mathcal{A}_{\mathrm{FS}}$ to obtain the tag's previous secret keys when $\mathcal{A}_{\mathrm{FS}}$ corrupts the tag. ***FS*** is defined using the game $\mathcal{G}_{\mathrm{FS}}$ played between a malicious adversary $\mathcal{A}_{\mathrm{FS}}$ and a collection of reader and tag instances, in which $\mathcal{A}_{\mathrm{FS}}$ interacts with the reader and with tags for an arbitrary period of time determined by $\mathcal{A}_{\mathrm{FS}}$. $\mathcal{A}_{\mathrm{FS}}$ runs the game $\mathcal{G}_{\mathrm{FS}}$ whose setting is as follows.

Phase 1 (Learning): $\mathcal{A}_{\mathrm{FS}}$ is able to send any **Execute**, **Send**[1], **Send**[2], **Send**[3] and **Corrupt** queries at will.

Phase 2 (Challenge): $\mathcal{A}_{\mathrm{FS}}$ starts a new session i, during which $\mathcal{A}_{\mathrm{FS}}$ chooses a fresh tag $\mathcal{T}$ to be challenged and sends it a **Corrupt** query to obtain its secret key x^i. Fresh means that the tag has not been issued any **Corrupt** query before.

Phase 3 (Guessing): Eventually, $\mathcal{A}_{\mathrm{FS}}$ terminates the game simulation and outputs $x^{t'}$ ($t < i$), which is its guess of the value of the previous key x^t of $\mathcal{T}$. Note here that $x^i = Update^{i-t}(x^t, t, \cdot)$[2].

The goal of $\mathcal{A}_{\mathrm{FS}}$ is to guess the correct value of x^t. The success of $\mathcal{A}_{\mathrm{FS}}$ in winning $\mathcal{G}_{\mathrm{FS}}$ and thus breaking the notion of ***FS*** is quantified in terms of $\mathcal{A}_{\mathrm{FS}}$'s advantage in guessing the correct value of the previous key x^t of $\mathcal{T}$. This is denoted by $Adv_{A_{FS}}^{FS}(k)$ where k is the security parameter. Hence, our concrete definition of ***FS*** is given as follows:

A protocol in an RFID system with security parameter k is forward secure if:

$$Adv_{A_{FS}}^{FS}(k) = \Pr[A_{FS}{}^{E,S,C} \quad win\, G_{FS}]$$
$$= \Pr[x^{t'} = x^t \,|\, x^i = Update^{i-t}(x^t, t, \cdot)]$$
$$\le \varepsilon(k) \quad ,$$

where $\varepsilon(k)$ is negligible function of k.

4. Security Analysis of the Anonymous RFID Authentication Protocol

4.1. Review of the Anonymous RFID Authentication Protocol

The anonymous RFID authentication protocol proposed by Shen et.al [1] is depicted in Figure 1. All the used notations are showed in Table 1. Even though the paper [1] provides strong privacy and security with low computation and communication cost, there are still two vulnerabilities under the above security model.

[2] *Update* denotes some key updating function.'·' denotes some related input of function *Update*.

Table 1. Notations

Symbol	Description
$\mathcal{R}$	RFID reader
r_R	Random number generated by RFID reader $\mathcal{R}$
$\mathcal{T}$	RFID tag
r_T	Random number generated by RFID tag $\mathcal{T}$
ID	Static identity of RFID tag $\mathcal{T}$
P	Pseudonym of RFID tag $\mathcal{T}$
S	Safeguard of P
x_T	Secret for RFID tag $\mathcal{T}$
BS	Back-end server
$h(\cdot)$	One-way hash function: $\{0,1\}^* \rightarrow \{0,1\}^l$
$\oplus$	Exclusive-OR (XOR)

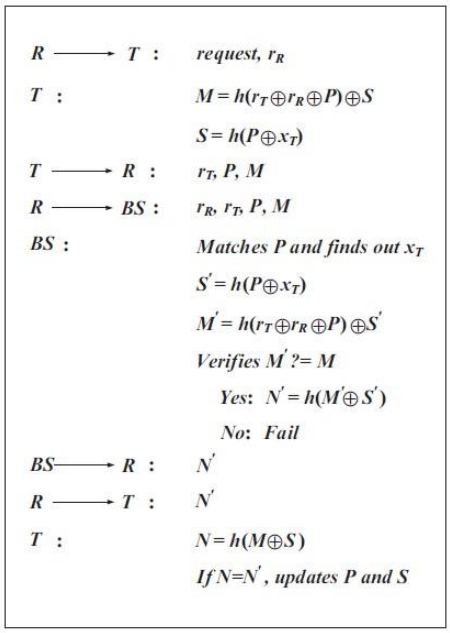

Figure 1. The Anonymous RFID Authentication Protocol

4.2. Security Analysis

1) Violation of untraceability

Let i be the protocol session. Let us assume that the adversary breaks into the tag's memory at time i. The adversary sends **Corrupt** query thus gets $x_T^{\,i}$. It then follows the protocol and waits for the tag memory to get updated to $x_T^{\{i+1\}}$. Note that, the adversary did nothing after getting $x_T^{\,i}$ and allowed the tag to continue and complete the protocol with the server for the session. After the tag memory has been updated to i+1, the adversary accesses the memory and gets $x_T^{\{i+1\}}$ at session i+1. Moreover, the adversary has got the protocol transcripts of session i ($r_R^{\,i}, r_T^{\,i}, P^i, M^i, N'^i$) via the public channel. Now, the adversary can compute the following: $\mathrm{ID} = x_T^{\,i} \oplus x_T^{\{i+1\}} \oplus M^i$. Thus, the ID of the tag is revealed. Next, the adversary has got the protocol transcripts of session i-1

($r_R^{\{i-1\}}, r_T^{\{i-1\}}, P^{\{i-1\}}, M^{\{i-1\}}, N'^{\{i-1\}}$) via the public channel. From this, the adversary can compute: $x_T^{\{i-1\}} = x_T^{\,i} \oplus M^{\{i-1\}} \oplus \mathrm{ID}$. Thus, the forward security is broken. Once the ID is revealed, the tag is no more anonymous and no more resistant to tracking. Thus, the protocol violates the tag untraceability.

2) Violation of de-synchronization

The proposed protocol is not fully resistant to de-synchronization attacks as well. Let us assume that at some point the adversary has blocked the two consecutive N' values (N' of two consecutive sessions). The server has thus already updated itself, but the tag has not. The tag and the server will remain de-synchronized from then. Let us elaborate the above scenario:

At session *i*, the tag has $x_T^{\,i}$. The server has $x_T^{\{i-1\}}$, $x_T^{\,i}$. Tag has been authenticated successfully. The server updates its memory to $x_T^{\,i}$, $x_T^{\{i+1\}}$. The adversary has blocked N'^{i}. So, the tag cannot update its memory. The tag still has $x_T^{\,i}$ in its memory. At session *i*+1, the tag has $x_T^{\,i}$. The server has $x_T^{\,i}$, $x_T^{\{i+1\}}$. Tag has been authenticated successfully using $x_T^{\,i}$. The server updates its memory to $x_T^{\{i+1\}}$, $x_T^{\{i+2\}}$. The adversary has blocked $N'^{\{i+1\}}$. So, the tag cannot update its memory. The tag still has $x_T^{\,i}$ in its memory. At session *i*+2, the tag has $x_T^{\,i}$. The server has $x_T^{\{i+1\}}$, $x_T^{\{i+2\}}$. Hence, tag cannot be authenticated successfully since the server does not have $x_T^{\,i}$ in its memory anymore. The tag and server get de-synchronized.

5. Conclusion

In this paper, we consider privacy issues in RFID system where the authorized readers must be able to identify tags without an adversary being able to trace them, and provide a formal security model for privacy in RFID system. Under this model, we analyze the recently proposed RFID authentication protocol named anonymous RFID authentication protocol and show attacks on them that compromise the privacy. In particular, the attacks like de-synchronization are very difficult to prevent. We can assume that the attacker can only block the transmission only one time to achieve this requirement. In addition, forward privacy is very important to protect the history output. In the future, we want to define a more general model to analyze the RFID authentication protocols with formal security proofs.

Acknowledgements

This work is supported in part by the research fund from Nanjing University of Information Science and Technology (Grant No. S8113003001), National Natural Science Foundation of China (Grant No. 61232016), National Basic Research Program 973 (Grant No. 2011CB311808), and the Priority Academic Program Development of Jiangsu Higer Education Institutions fund. It was also supported by the Industrial Strategic Technology Development Program (10041740) funded by the Ministry of Knowledge Economy (MKE) Korea, and by the Natural Science Foundation of Jiangsu Province (No. BK2012461).

References

[1] J. Shen, D. Choi, S. Moh and I. Chung, "A Novel Anonymous RFID Authentication Protocol Providing Strong Privacy and Security", 2nd Int. Conf. on Multimedia Information Networking & Security (MINES 2010), IEEE Press, **(2010)**, pp. 584-588.
[2] G. Avoine, "Adversarial Model for Radio Frequency Identification", Cryptology ePrint Archive, report 2005/049, **(2005)**.
[3] A. Juels and S. A. Weis, "Defining Strong Privacy for RFID", IEEE PerCom'07, **(2007)**, pp. 342-347.
[4] T. V. Le, M. Burmester and B. Medeiros, "Universally Composable and Forward-Secure RFID Authentication and Authenticated Key Exchange", ASIACCS'07, **(2007)**, pp. 242-252.
[5] S. Vaudenay, "On Privacy Models for RFID", Advances in Cryptology – Asiacrypt'07, LNCS 4833, **(2007)**, pp. 68-87.
[6] M. R. Rieback, B. Crispo and A. S. Tanenbaum, "The Evolution of RFID Security", IEEE Pervasive Comp., vol. 5, no. 1, **(2006)**, pp. 62-69.
[7] A. Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, **(2006)**, pp. 381-394.
[8] I. Coisel and T. Martin, "Untangling RFID Privacy Models", Journal of Computer Networks and Communications, vol. 2013, **(2013)**.

Authors

Jian Shen Jian Shen received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2007 and the M.E. and Ph.D. degrees in Computer Science from Chosun University, Gwangju, Korea, in 2009 and 2012, respectively. Since late 2012, he has been a faculty member in the School of Computer and Software at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include computer networking, security systems, mobile computing and networking, ad hoc networks and systems, and ubiquitous sensor networks.

Wenying Zheng received the B.E. degree from Yanbian University, Yanji, China, in 2007 and the M.E. degrees in Electronic Engineering from Chosun University, Gwangju, Korea, in 2009, respectively. Since late 2012, She has been a faculty member in the School of Applied Meteorology at Nanjing University of Information Science and Technology, Nanjing, China. Her research interests include image security, image recognition, and security systems.

Jin Wang received the Ph.D. degree in the Ubiquitous Computing laboratory from the Computer Engineering Department of Kyung Hee University Korea in 2010. Now, he is a professor in the Computer and Software Institute, Nanjing University of Information Science and technology. His research interests mainly include routing protocol and algorithm design, performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.

Zhihua Xia received his BE in Hunan City University, China, in 2006, PhD in computer science and technology from Hunan University, China, in 2011. He works as a lecturer in School of Computer & Software, Nanjing University of Information Science & Technology. His research interests include Steganography and Steganalysis, digital forensic, image processing, and pattern recognition.

Zhangjie Fu received his BS in education technology from Xinyang Normal University, China, in 2006; received his MS in education technology from the College of Physics and Microelectronics Science, Hunan University, China, in 2008; obtained his PhD in computer science from the College of Computer, Hunan University, China, in 2012. Currently, he works as an assistant professor in College of Computer and Software, Nanjing University of Information Science and Technology, China. His research interests include digital forensics, network and information security, copyright protection technology.