Electronic Invoice Authenticity Verifying Scheme Based on Signature Recognition

Rongna Xie¹, Weihua Mao¹, Guozhen Shi¹

¹Beijing Electronic Science and Technology Institute, 100070 Beijing, China

Abstract. With the rapid development of network and information technology, paperless and electronics have become the development trend of today's economic life. As a consumption certificate, e-invoice has become more and more demanding in e-commerce. The existing electronic invoice verification method only judges whether the electronic invoice has passed the verification by verifying the authenticity of the digital signature of the seller. Although the verification result has certain reference value, it is assumed that the electronic invoice does not authorize by the tax authority, because the verification process will not verify the signature of the tax authority, which cannot be detected as an illegal behavior. This verification method cannot guarantee the complete legality and authenticity of the electronic invoice. Aimed at the above problems, this paper designs a digital signature-based electronic invoice authenticity verifying scheme. By verifying the legality of the signature of the seller and tax authority, and the truth of the trading information, it can ensure the authenticity of the electronic invoice passed.

1. Introduction

In recent years, e-commerce, known as “commercial activities conducted through an exchange of information generated, stored, or communicated by electronic, optical, or analogous means...”[The United Nations Commission on International Trade Law, UNICTRAL][1], has experienced rapid development in our daily lives. In 2016, the total transaction amount of e-commerce in China reached 28.9 trillion. Compared with 20.8 trillion in 2015, it increased by 38.9%. In the past five years, the average annual growth rate of China's e-commerce transaction amount reached 38.2%[2].

Due to some sound feature, such as able to provide 7*24 service, fast access[3], no geographical restrictions, shortening the commercial supply chain, e-commerce got a quick promotion in the fields of tourism, catering, entertainment, and shopping. E-commerce is providing us with fast, safe full and convenient service, but also brings new challenges. The challenge of payment certification technology is one of them and verifying the payment voucher effectiveness is one of the key issues. The validation of the payment voucher is a convenient and efficient way to ensure the authenticity of the voucher.

Traditional paper invoices are the most commonly used payment vouchers. Paper invoices are printed with special paper for anti-counterfeiting, which makes it more difficult and reduces the possibility of falsify invoice. However, the issuance of paper invoices not only consumes a large amount of special paper but also generates a certain transportation cost. In the invoice reimbursement process, the reimbursement staff needs time to verify the invoice and paste the invoice; the accounting staff needs to spend a lot of time to check the invoice content, verify the authenticity of the invoice, and the manual verification is prone to errors, resulting in low efficiency and high error rate. Paper invoices from invoicing, billing, reimbursement, and accounting will consume a lot of resources and
labour costs, and the time period is long, which obviously cannot meet the needs of the rapid development of society at this stage. In contrast, the issuance, approval, and delivery of e-invoices are all completed by computer systems. Making query and reimbursement are more convenient. The use of e-invoice is conducive to saving social resources, reducing invoice management costs and improving economic efficiency [4]. The promotion and use of e-invoice can effectively solve the problems of verification of paper invoices, high labour costs and long time periods, which meet the needs of the e-commerce market under the rapid development of Internet technology.

In order to solve the security risks such as fraud, fraudulent use, tampering, and stringing in the invoice, the authenticity and content integrity of the invoice information must be ensured during the use of the electronic invoice. The “source authenticity” means that there is a clear seller or the invoice issuer, “content integrity” means that the required invoice content has not been modified [5]. How to ensure the authenticity and integrity of e-invoice is the core issue that needs to be solved in electronic invoice verification, and it is also the key to the safe use of e-invoice.

The rapid development of e-commerce has prompted consumers to become more and more demanding for e-invoice. Some areas or enterprises have begun to provide e-invoice, but the scope of promotion and use of e-invoice is still small, mainly because the verification is difficult [6]. The recognition of e-invoice by enterprises or units is low. Efficient verification is an important guarantee for the widespread use of e-invoice. It solves the problem of authenticity verification, the promotion and use of e-invoice can grow rapidly.

In view of the above problems, this paper proposes an authenticity verification scheme for e-invoice based on signature verification, which can verify the legality and authenticity of e-invoice. The program extracts information from the invoice itself, verifies the identity of the tax agency in the verification process, ensures that the invoice is issued by the tax authority, and verifies the compliance of the invoice information to ensure that the invoice issued is in the business scope of the enterprise. Within the validity period of the invoice, verifying the invoice content and the signature of the issuing party, you can determine that the triple verification guarantees the correctness of the verification result. The verification of e-invoice can be combined with the payment system or the sales system to fundamentally eliminate the use of invoices to evade tax evasion.

The following sections of the paper are organized as follows. Section 2 introduces the research results of other scholars in the field of electronic invoicing, discusses their advantages and disadvantages and compares them with the scheme of this paper. Section 3 introduces the principle of generating e-invoice. In section 4, the authenticity verification scheme of electronic invoice is discussed in detail, and the design principle is analysed. Section 5 analyzes the security of the invoice verification scheme and proves that this scheme can verify the legality and authenticity of the electronic invoice. Section 6 summarizes this article.

2. Related Work
E-invoices are invoices that are generated, processed, stored, and mailed in electronic form [7]. The verification of an electronic invoice is to verify the legality, authenticity, and integrity of the invoice. The verification method is closely related to the process of generating the electronic invoice. The method of generating the electronic invoice can infer the verification method of the electronic invoice and the perfect electronic invoice verification scheme. It can also guide the generation of e-invoice.

At present, the application of e-invoice in Northern Europe and Chile is developing rapidly. Most countries in Europe and America have established an e-invoice operation system [8]. Most foreign e-invoices use digital signature technology and user information and bank binding identification [9-10]. China's e-invoices are in the development stage, large enterprises started to apply several years ago, but SMEs use less.

Spanic [11] proposed an electronic invoicing system that can serve different users. The system uses digital signature technology in the process of generating e-invoice so that both parties can not deny the transaction. Concerning data integrity, digital signature and time stamp technology are used to ensure that e-invoice cannot be transferred during storage. The legality of the invoice is controlled by the
digital signature and the private key to verify the authority of the login system, but the validity of the invoice cannot be determined from the information of the invoice itself.

Netter [12] proposed a security mode for e-invoice, which classified the security of e-invoice into three methods: generation, storage, and transmission. The use of the access control method for the storage of invoices, and digital signature technology to protect the integrity of the invoice, and a secure channel for transmission, to ensure the security of the transmission and reception process. The program protects the entire lifecycle of e-invoice, ensuring the integrity of e-invoice, and is not easily lost or illegally accessed. However, the program cannot verify the legality of e-invoice.

In China, Hongyang Chu [13] proposed a data-oriented electronic invoice framework. The scheme uses digital signature technology in the anti-counterfeiting of e-invoice. That is, in the process of generating e-invoice, the electronic invoice template data of adding transaction information is signed, to ensure the integrity of the invoice and ensure the transaction. However, the electronic invoice generated by the scheme is not signed by the tax authority, and the legality of the electronic invoice template used cannot be guaranteed. The verification of the electronic invoice generated by the scheme cannot confirm the legality of the electronic invoice issuing institution.

The several above schemes use digital signature technology in the process of generating e-invoice. This signature is the signature of the seller or the sender, which can guarantee the non-repudiation of the parties and the integrity of the invoice, but the invoices are not verified. The legality of the signature of the tax agency, therefore, can not guarantee the legality of the electronic invoice, there is the possibility of forging invoices.

The existing electronic invoice verification scheme is still the traditional thinking: the verification of the invoice is to convert the information on the paper invoice into electronic information, then analyze it, verify whether the submitted information is correct, or check the invoice whether the authenticity and the stamp are valid is essentially the comparison of information. Effective verification requires signature verification of the electronic invoice to verify the authenticity and validity of the invoice.

3. The principle of generating e-invoice

3.1. Security requirement for e-invoice

The electronic invoice is the original transaction voucher [14], which contains a large amount of information of the buyer and the seller. Many of the information relates to trade secrets, which have important commercial value to the seller and the purchaser. If there is a problem due to the security of the electronic invoice, the information leaks or being stolen by a malicious third party will have a significant adverse effect on the parties involved. Therefore, in the process of using e-invoice, not only should it be convenient for all parties to use, but also ensure the security of e-invoice, and ensure that information is not leaked or stolen during the process of issuing, transmitting, storing and checking [15]. The electronic invoice generation process must have corresponding measures to ensure the integrity, uniqueness, and validity of the data. Even if there is a problem with the invoice, it can be discovered through the verification process.

3.2. The process of generating e-invoice

The information of the electronic invoice is determined by the specific content of the transaction parties and the transaction. A complete electronic invoice requires the basic information of the seller and the basic information of the buyer to determine the stakeholder of the invoice, as well as the date, amount, project name, etc. The transaction information clarifies the transaction content and also requires the signature of the tax agency and the signature of the seller to make a ruling in case of dispute. Then the electronic invoice generation system should have the following information on the electronic invoice automatically generated based on the transaction information:

Transaction information: including transaction date, e-invoice number, e-invoice code, check code, and also has the order number, machine code, and other information.
Product information: including the category name, specification model, unit, quantity, price, tax rate, tax payable, total amount payable, of the goods sold.

Seller information: including the name of the seller, the taxpayer identification number, the address phone number, the bank account and the account number, the name of the biller, the payee and the reviewer.

Consumer information: including the name, taxpayer identification number, address, phone number, account bank, account number, where the name and taxpayer identification number must be filled in, the address phone number and the account bank account information can be optionally filled out.

The ordinary e-invoice generation process is shown in Figure 1. The transaction information is converted into a standard format and added to the electronic invoice template, and then the seller signs it to form a valid electronic invoice.

The authority of the electronic invoice generated in this way cannot be determined. If the electronic invoice template used is not issued by a tax authority, the criminals can easily imitate the electronic invoice template and issue a fake invoice. The traditional paper invoices are used to prevent invoice fraud and tax evasion. The invoice has not only the official seal of the seller but also the official seal of the tax authority. Like the paper invoice, the electronic invoice not only requires the seller but also the tax agency signature.

To ensure the legality of the electronic invoice, the tax authorities should sign the electronic invoice template to generate an authoritative blank electronic invoice to prevent fraud. After the transaction information is added, the seller signs it to generate a valid e-invoice. The improved e-invoice generation process is shown in Figure 2. The specific process is as follows:

1) Sales apply for e-invoice to the tax authorities.
2) The tax authority develops an electronic invoice template, and the ticket information in the template includes electronic invoice number, electronic invoice code, electronic invoice name, quota and other information.

3) The tax authority verifies the ticket information on the template, and after confirming the correctness, sign the ticket information and the public key of the tax authority with the private key $s_r = \text{Sig}(sk_r, m_i \parallel pk_r)$, generate a blank e-invoice, where $s_r$ is the signature of the tax agency, $m_i$ is the electronic invoice initial information, and $pk_r$ is the public key of the tax agency.

4) After the transaction occurs, the consumer submits the invoice header information, and the seller adds the transaction information to the blank electronic invoice to generate the initial electronic invoice.

5) The seller checks the transaction information, the seller information, and the consumer information. After confirming the correctness, the private key is used to sign the transaction information, the ticket information on the blank invoice, the tax authority public key, and the seller's name to generate a valid e-invoice $s_s = \text{Sig}(sk_s, m_2 \parallel (m_1 \parallel pk_s))$, which $s_s$ is the signature of the seller, $m_2$ is the transaction information, and $sk_s$ is the seller's private key.

4. Electronic invoice verification scheme

4.1. Description of the verification scheme

The authenticity verification of e-invoice requires verification of the legality and authenticity of the invoice. The verification of the general electronic invoice realizes the information inquiry function of the electronic invoice, and the item purchased by the individual can check whether the amount is correct, but cannot detect whether the electronic invoice is legal. For the e-invoice reimbursed by the unit, the accounting staff not only needs to check the amount but also needs to judge whether the electronic invoice has been tampered with. The verification process needs to check the legality, authenticity, and integrity of the electronic invoice, and only verify that the invoice information is correct and cannot meet these requirements. To verify the authenticity of an electronic invoice, it is necessary to verify the correctness, completeness, and innocent modification of the information carried in the electronic invoice.

To verify the authenticity of the electronic invoice, it is necessary to ensure the accuracy, completeness and innocent modification of the three types of information, such as transaction information, consumer information, and seller information, and these three kinds of information need to be verified. The existing electronic invoice inspection platform only provides the inquiry function, and queries the database of the invoices of the merchant through the invoice number, the invoice code, date, and the check code, but does not implement the verification function.

The electronic invoice verification scheme designed in this paper first carries out the legality verification of the signature of the tax agency, then verifies the signature of the seller, and finally verifies the compliance of the transaction information content.

4.2. Specific process

The verification scheme is mainly divided into two parts, the verification of the blank electronic invoice and the verification of the valid electronic invoice. The verification process is described as follows.

Step1: The user initiates a verification request to the e-invoice verification client and submits the e-invoice information.

Step2: Verify the legality of blank e-invoice.

2-1: The verification platform extracts the key information of the blank e-invoice, including the tax institution public key $pk_e$, the tax agency signature $T_s$, and the initial information $m_i$.

2-2: Verify that the tax authority's public key $pk_e$ is valid. The correctness of the tax authority's public key $pk_e$ can be verified by querying the public key list, and the correctness of the tax authority's
public key $pk_t$ can also be verified by a digital certificate. If the verification is passed, proceed to the next step. If the verification fails, then query the latest tax authority public key and the past public key.

2-3: Verify the correctness of the tax agency's signature $T_{sk}$ with the tax agency private key $T_{sk}$.

If the verification is passed, it means that the blank e-invoice is indeed issued by the tax authorities and has not been tampered with. If the verification fails, the signature of the tax authority $T_{pk}$ has been verified, and the signature is not authorized by the tax authority. The invoice is fake, please jump to Step4, and return invalid invoice results.

Step3: Verify the authenticity of the valid invoice.

3-1: Extract the key information on the valid e-invoice from the e-invoice, including the transaction content information $m_1$, the seller's public key $Spk$, and the seller's signature $S_{sk}$.

3-2: Verify that the seller's public key $Spk$. By verifying the correctness of the seller's public key by querying the public key list, the correctness of the seller's public key can also be verified by the certificate. If the verification is passed, proceed to the next step. If the verification fails, the latest public key of the seller and the past public key are queried.

3-3: Verify that the seller's signature $S_{sk}$ is correct with the seller's private key $S_{sk}$.

If the verification is passed, the compliance verification is performed. If the verification fails, the seller's signature has been tampered with, and the process returns to Step 4 and returns the invalid invoice result.

3-4: Verify the compliance of the transaction content information. Verify that the amount issued by this e-invoice is within the allowable amount, verify that the date of the invoice is within the validity period, and verify that the business type of the invoice complies with the regulations. If the verification is passed, the invoice is determined to be a valid invoice, and the valid invoice verification result is returned. If one or more verification errors occur, the invoice is determined to be an invalid invoice, and the next step is performed to return the invalid invoice result.

Step4: Verify platform to return the verification result to the client.

Step 5: The client returns the final verification result to the user and displays, and the authenticity verification of the e-invoice is completed.

5. Security analysis

5.1. Reliability

1) Unforgeability

The unforgeability of the signature algorithm ensures that the attacker cannot tamper with any information on the invoice, and only the tax authority and the seller can generate a valid signature with the private key. Even if the attacker wants to tamper with the information on the invoice, the attacker does not have a tax authority private key, and the corresponding signature cannot be formed. When the public key is used to verify the seller's signature, the falsified invoice can be identified.

Even if the attacker forged an invoice with a real blank invoice, without the seller's private key, the corresponding signature could not be generated, and the forged invoice could be found during the verification of the signature.

2) Integrity

The complete e-invoice includes the seller information, the consumer information, date, amount, business type, transaction details, tax agency signature, and seller's signature. It is known from unforgeability that invoices cannot be tampered with or forged. The above information is required for the verification process. Information gaps are also illegal invoices. The entire verification process ensures the integrity of the invoice.

3) Trackable

The fraudulent behavior of e-invoices includes non-tax authorities issuing invoices, invoices issued by non-sellers, errors in transaction details, exceeding the expiration date, and business types not matching. For each generated link that is likely to be fraudulent, the verification process has been
verified accordingly, and which verification process cannot be passed, indicating that there is a problem in this link, and it is easy to trace the source of the problem.

5.2. Effectiveness

1) Legality

Legitimacy refers to compliance with the national tax system and recognized by the tax authorities. In the verification process, the legality of the blank invoice is verified by verifying the signature of the tax agency. The verification proves that the invoice is issued by the taxation agency and the invoice recognized by the state taxation department. It is legal to determine the invoice from the national taxation system. If the verification fails, it means that the invoice is not issued by the tax authority, it is an illegal invoice, and the plan can ensure that the verification is passed as a legal invoice.

2) Timeliness

Invoice authenticity verification: the main time consumption is the information extraction time, verifying whether the tax agency public key is valid, that is, one signature verification time.

Invoice validity verification: the main time consumption is the information extraction stage, verifying whether the seller's signature is valid, that is, one signature verification time.

In each verification process, the invoice verification scheme of this paper calls a total of two signature verification algorithms. The steps are simple, the verification efficiency is high, and the response time can be shortened.

3) Universality

This document verifies the full content of possible fraudulent e-invoice, and the verification principle applies to all types of e-invoice. The verification scheme is an improvement on the existing e-invoice generation scheme and applies to the existing electronic invoicing system.

6. Conclusion

The development of e-commerce has made the demand and application of e-invoice more and more extensive, but the inspection of e-invoice is only through the invoice number, invoice code, transaction date and other information to query the e-invoice in the tax agency database to compare the invoice that needs to verify with the information obtained. The authenticity and integrity of the e-invoice are not verified from the data of the invoice itself, and the fraudulent behavior of the illegal invoice cannot be found. The e-invoice verification scheme designed in this paper extracts information from the e-invoice itself, verifies the signature of the invoice tax authority to verify the legality of the invoice, verifies the seller's signature and transaction information to ensure the authenticity of the invoice, and the three verifications can determine the e-invoice for verification - authenticity, integrity, and legitimacy.

Acknowledgement
This work is supported by The National Key Research Program of China (2017YFB0802705)

References
[1] Hill R, Walden I. The draft UNCITRAL model law for electronic commerce: issues and solutions[J]. Computer Lawyer, 1996, 13(3): 18-22.
[2] Hongfei Y. National report on e-commerce development in China[J]. United Nations Industrial Development Organization, Inclusive and Sustainable Industrial Development Working Paper Series, WP17, 2017.
[3] Junyong X, Linbo J. Electronic commerce in China: current status, development strategies, and new trends[J].
[4] Humski L, Vrdoljak B, Skocir Z. Concept, development and implementation of FER e-invoice system[C]/ SoftCOM 2012 - 20. International Conference od Software, Telecommunications & Computer Networks / Rožić, Nikola ; Begušić, Dinko. 2012:1-5.
[5] Bofeng X, Xiaoyou L. Reference and Enlightenment of the Electronic Invoice in the EU and Taiwan District[J]. International Taxation in China, 2016 (7): 70-74.

[6] Joung Y J, Tseng Y C, Cha S C, et al. Motivations, Deployment, and Assessment of Taiwan’s E-Invoicing System: An Overview.[C]// Hawaii International Conference on System Sciences. IEEE Computer Society, 2014.

[7] European Commission. "European Electronic Invoicing (EEI) Final Report." European Commission Informal Task Force on e-Invoicing, 2007.

[8] CHAI Yueting, YU Xiao, HUANG Yadong. Electronic invoice management and public service system. Journal of Tsinghua University(Science and Technology), 2018, 58(6): 598-602.

[9] Ponnapalli H K B, Saxena A. A Digital Signature Architecture for Web Apps[J]. It Professional, 2013, 15(2):42-49.

[10] Chuchaisri P, Newman R E. Multi-resolution elliptic curve digital signature[C]// IEEE, Conference on Local Computer Networks. IEEE Computer Society, 2012:93-101.

[11] Španić D, Ristić D, Vrdoljak B. An electronic invoicing system[C]// International Conference on Telecommunications. IEEE, 2011:149 - 156.

[12] Netter M, Pernul G. Integrating Security Patterns into the Electronic Invoicing Process[C]// International Workshop on Database and Expert Systems Application. IEEE, 2009:150-154.

[13] Chu H, Chai Y, Liu Y, et al. A novel E-Invoice Framework towards data-oriented taxation system[C]// IEEE, International Conference on Computer Supported Cooperative Work in Design. IEEE, 2014:242-246.

[14] Linde S, Hansen B. KEY FACTORS FOR THE ADOPTION AND SUBSEQUENT USE OF E-INVOICING[J]. Academia Revista Latinoamericana De Administración, 2012, 111(50):15-30.

[15] Matus A, Guerra E, Fuertes W, et al. On the development of an electronic invoicing solution to integrate SMEs with a tax-collection egovernment-platform[C]// Fourth International Conference on Edemocracy & Egovernment. IEEE, 2017:94-101.