Research Journal of Applied Sciences, Engineering and Technology 7(5): 908-915, 2014
DOI:10.19026/rjaset.7.334
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 24, 2012 Accepted: January 01, 2013 Published: February 05, 2014

Research Article

Research of Cryptographic Algorithms Applied in Electronic Commerce

Cheng Zengping and Chen Yanshou
Hubei University of Automotive Technology, ShiYan City, Hubei Province 442000, China

Abstract: With the developments of network communication, electronic commerce plays a more and more role in the trade business and industry structure. The requirement for the electronic commerce turns to be higher. In this study, we study current status about the cryptographic algorithms exploited in electronic commerce. We discuss the advantages and disadvantages about the symmetric and asymmetric algorithms and improve them. Then we give a new scheme that combines the improved symmetric algorithm and asymmetric algorithm. We give sound reasons to explain why our scheme is more secure. Finally, we carry the experiments to show the security of our scheme.

Keywords: AES, asymmetric algorithm, electronic commerce, key, RSA, symmetric algorithm

INTRODUCTION

Electronic commerce is a fundamental approach for economic globalization and trade liberalization. It also motives the reformation and technique progress for the traditional industry structure. Electronic commerce has made a huge change for the way of economic execution with its amazing power since twenty century. Now, with the rapid growth of computer network and communication technique, the development of electronic commerce is flourishing. As a new business mode, electronic commerce is the most primary trend in the future and plays an important role in people's life. Electronic commerce is the method of using any information and communication technique to take the business action, manage the execution and exchange the information. From the point of technique, the development of electronic commerce can be divided into three parts. First is traditional electronic commerce. Second is Electronic Data Exchange (EDI). Third is Web/Browser electronic commerce. Now it is on its way to the step of intelligent electronic commerce.

Most of the researches on electronic commerce focus on the implementation of data exchange. The issue of assuring the security of the data does not obtain enough attention it deserves in the past. With the generation of more and more challenges in the web circumstance, ignoring the security issue will lead to the leakage of secret information and sense information. So the level of security is a key factor that influences the existence of electronic commerce.

The security issues about electronic commerce include information security, credit security, security managements and law assurance. The security requirements that can defend against different threat of attacks can be summarized as follows: confidence, integrity, availability and un-deniability. The transmission scheme of XML is adding the cipher texts of the encrypted or signed message into the original file according to the standard of XML data security and transferring this new XML file together with the original one. When the encryption algorithm and signature algorithm are secure, this kind of transmission scheme can guarantee the encryption and signature of the XML carefully and no problem about data security will rise up.

However, with further cryptanalysis, many algorithms widely used in above scheme are broken theoretically or practically. In 2004, one of the most well-known hash functions MD5 is practically broken by Wang *et al.* (2005b). Wang *et al.* (2005a) broken SHA-1 hashes function, which is used in the field of electronic commerce in US. Both of these two hash function are the basic primitives of the electronic signature schemes in the world, which are widely used in the fields of finance, bond and so on.

Another important primitive being broken is DES, which is the previous standard of symmetric cipher in US. DES is designed by IBM and is approved as FIPS-46 standard in 1977. The key length of DES is only 56 bits, which is far from secure under today's computation ability. The full version of DES is broken by Matsui with linear cryptanalysis in 1993 (Mitsuru, 1993). However, previous many protocols for electronic commerce, such as SSL and SET, are based on DES.

The breakthrough of cryptanalysis in above algorithms means that an authorized signature can be forged, so that the confidence and integrity are destroyed. Actually, with the collision found by Wang *et al.* (2005a) Lenstra forged the digital signature that

Corresponding Author: Cheng Zengping, Hubei University of Automotive Technology, ShiYan City, Hubei Province 442000, China

satisfies the standard of X. 509. MD5 is broken not only in the theoretical term, but also in the practical term.

As mentioned above, the cipher texts are stored in the original XML file and used together. So once the whole XML file is obtained or copied illegally, the XML file will be obtained by non-authorized users due to the flaws of the encryption or signature algorithms.

In 2000, National Institute of Standards and Technology (NIST) proposed a new standard for block ciphers. After a series of analysis and evaluation, Rijndael is chosen as the final AES. This gives more insight on the security application of electronic commerce. Researchers began to consider replacing DES with AES (Daemen and Rijmen, 1998; Khiabani and Shuangqing, 2011) for a high security margin. However, in the most recent result about AES, Rijndael has been theoretical broken by Bogdanov *et al*. (2011). another analysis on AES include (Yongzhuang *et al*., 2011; Jiqiang, 2011). Though this will not lead to a practical threat, we still recommend a safer scheme for using in a long period.

In this study, we study the latest security issues on the economic commerce, especially about the symmetric algorithms and asymmetric algorithms. We investigate the disadvantages about both of these two kinds of algorithms. Then we design a more secure digital signature scheme by combining the AES algorithm and the RSA algorithm with a new way. We construct the symmetric algorithm by using the AES as a basic module, which provides a higher provable security margin. By applying this new kind of data encryption method in the economic commerce, we achieve a safe data transmission, an examination for data integrity and digital signature.

CURRENT STATUS ABOUT ELECTRONIC COMMERCE AND ITS SECURITY

Security of electronic commerce based on XML: EBXML is proposed by UN/CEFACT and OASIS in 2001. Its purpose is to construct an electronic commerce structure based on an open XML standard. This will provide a transparent, secure and unified situation of the electronic data exchange for the electronic commerce trade in the world. This is also for simplifying the trade procedure.

The web service based on XML technique is a new kind of distributed computing model. The basis of WS is XML, SOAP, WSDL, UDDI. XML helps the applications to exchange the data and service. In 2002, IBM and Microsoft issue the “Security in a web service world: a proposed architecture and roadmap”, which describes the security standard in the circumstance of web service.

The security techniques of XML include: XML encryption, XML digital signature, XML key managements XKMS, XACML, SAML. XML Encryption Syntax and Processing is developed by W3C and is issued also in 2002. This standard describes the encrypting process of the data and the results represented by XML. The data can be XML files, XML elements and the content of XML elements.

The primary purpose of XML encryption is as follows. First is to support the encryption for any kinds of digital content, including XML files. Second is to assure that any non-authorized users cannot have access to the data in a transmission or in the storage. Third is to keep the security in each step of data processing, even when the data is staying at some specified point. Fourth is to express the data with XML. XML Signature Syntax and Processing (RFC3275) is developed by the W3C and IETF and has become W3C recommendations for organizations. The latest version was released in February 2003. This specification describes the XML representation of the digital signature and verifies the digital signature process of XML representation. XML signature provides a flexible signature mechanism; not only to support the network resources and the signature of the message, but also to support part of an XML document or message to be signed. It also supports the public-key digital signature and the hash verification code with symmetric key.

As mentioned before, the risk of traditional data transmission mode appears when the cipher text data is stored in the original XML document and is transmitted together. When the entire XML document is intercepted or illegal copied, due to the defects of the existing encryption or signature algorithm, the XML document is get by illegal users.

Applications of cryptographic algorithms in electronic commerce: In order to guarantee the security of the electronic commerce requirements, the system must make use of security technology to provide reliable security services for the participants in the e-commerce activities, including: identification services, access control, confidentiality, non-repudiation services. Various services of electronic commerce security need to achieve. Electronic commerce uses security technology including: encryption, digital signatures, digital certificates, envelope.

Cryptographic algorithms are very important in electronic commerce. First, cryptographic algorithms are applied in the transmission. Various cryptographic techniques provide a guarantee for the safety of the common channel transmission for information in electronic commerce.

The implementation process of the cryptographic technology is a core primitive to protect the security of information. When the information in the common channel transmission is encrypted, the illegal thefts cannot decipher the information they obtain and get the plaintext. Thus the encrypted data does not make any sense for them. Most practical applications are used to combine the symmetric encryption algorithms and public key algorithms. The process is as follows:

Suppose that Alice has the original data P to be sent to the recipient Bob. The sender Alice uses a random number r as a key to encrypt the original data (using a symmetric encryption algorithm) and then uses the public key of the recipient B to encrypt the random number r. Finally, both of these two data are sent to Bob. Bob receives the encrypted data and decrypts this data with his own private key to obtain r. Then he uses r to do a decryption (using the symmetric decryption) to get the original message. Note that the symmetric encryption and decryption operations are only done with the random number r for the large message. The public key algorithm is only used for processing the random key r.

By this way, the advantage of the symmetric encryption algorithm (high speed) and the advantage of the asymmetric encryption (be convenient for the key management) are combined.

According to the theory of asymmetric encryption algorithm, a legal user will exploit a private key to decrypt the secret information, so one can take advantage of a person's public key to encrypt the information and send the encrypted information. Because others cannot know the private key, so the identity of this person can be completely determined. In order to create successful and secure electronic commerce activities, you need to establish an authentication system on the basis of an asymmetric digital certificate system. The public key digital certificate can be obtained for trading and other digital certificates issued by the authorized third party have high credibility. Currently, identity authentication based on PKI system aims for meeting the requirements of electronic commerce.

In order to maintain the confidentiality of the encryption algorithm, the original requirements for the confidentiality are not enough by today's standards. If a person of one organization leaks some secret algorithm, others in the same organization have to change their algorithms. This limits the standardization of cryptographic algorithms. Each organization must have its own unique algorithm for each user, so it is impossible to form an effective standard, using a common hardware and software products to achieve. The security of all of these algorithms is based on the security of the key rather than the details of the algorithm.

Message integrity and digital signature techniques: Besides the authentication, the purposes of electronic commerce security also include message integrity, non-repudiation and so on. Information integrity can be ensured through a single Hash function (HASH). First, send a message by calculating a hash value. For a message, the message itself and the hash value are then encrypted and sent to the recipient. After receiving the information, the recipient can decrypt the received information and calculate a hash value of the message. Then he compares the computed hash value with the received hash value. If both of them are the same one, the message will be regarded as without any change during the transmission. Otherwise, the message is considered being changed in the transmission process. The sender distributes the message to the recipient with a signature signed using his private key. The recipient who receives this message decrypts the message using the sender's public key and confirms the contents of the data packet. After confirmation of the message content, the recipient will use its private key to sign the approved information. The sender who receives the approval letter applies the recipient's public key to decrypt the data and save the identified data. The sender cannot deny that a message is from him because the recipient can use the sender's public key to check this.

Also, the recipient cannot deny that he has received this message, because it is decrypted using the recipient's public key.

Digital signature technology based on RSA algorithm in the application of electronic commerce can prevent the transaction process towel from forgery, falsification of information, or the fraudulent use of someone else that has sent a message, issuing a letter being received and then denying, etc. This is because that you cannot deny sending the message signature (i.e., anti-repudiation) after the sender with a private key has encrypted a message. Receivers take advantage of the signature packets sent by the sender and use the public key to verify the sender’s identity. Because the recipient do not know the sender's private key, it is impossible to forge the signature of the message sender (authenticity), or to steal the confidentiality or tamper (i.e., integrity). Therefore, the use of digital signature technology can effectively meet the information requirements of confidentiality, integrity, authentication and non-repudiation of delivery of the electronic commerce and effectively prevent security risks in a variety of electronic commerce transactions in information security.

RESEARCH OF SYMMETRIC ALGORITHM AND AES

Symmetric encryption algorithm: The so-called symmetric algorithm is encrypted and decrypted using the same user key. Firstly, the communicating parties

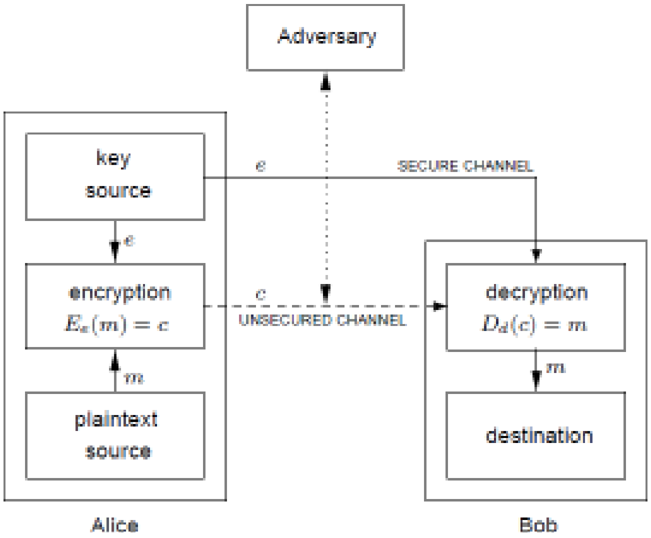

Fig. 1: The two-party communication channel exploiting symmetric-key encryption

must exchange the key used for the message. The sender exploits the key encrypt the information and transmit it. The recipient receives the information and uses the same key to decrypt the information. The well-known symmetric algorithms include DES, 3DES, IDEA, KASUMI, AES, Serpent, MISTY.

The advantages of the symmetric algorithms are as follows: Easy to implement in hardware; high speed in software, high confidentiality. There are a lot of software and hardware implementations and their corresponding improvements in the world.

Consider an encryption algorithm containing the sets of decryption and encryption transformations respectively, where K is the key space. The encryption scheme is said to be symmetric-key if for each key pair related to encrypting and decrypting key pair. It is said “easy” to determine one key from another. Since the decryption key is equal to the encryption key in most practical symmetric-key encryption schemes, the term symmetric key turns to be proper. Other terms used in the literature are single-key, one-key and private key.

A two-party communication channel exploiting symmetric-key encryption can be described by the Fig. 1. This figure shows both confidential and authentic channel. One of the major issues with symmetric-key encryption is to discover an effective approach to consent on and exchange keys safely. This question is regarded as the key distribution. It is supposed that all parties know the transformations of encryption process and decryption process. That is, the encryption scheme is known to them. As has been stress several times the only information that has to be required to be kept secret is the encryption master key. However, due to the property of symmetric-key, this means that the decryption key should be kept secret. The master key from encrypting process can generate the decryption key.

AES: In 2000, the Rijndael is chosen by NIST as the Advanced Encryption Standard (AES), as a replacement of DES for the US government. This new standard encryption algorithm has become one of the most widely used block cipher for the decade. It suffers a lot of cryptanalysis in the world, such as square attack, differential attack, impossible differential attack, differential-linear attack, meet-in-the-middle attack and so on. A considerable amount of these attacks apply the weaknesses of AES key schedule more or less. On the one hand, almost all the differential-type attacks can be put in a related-key model for a lower time and data complexity than in a single-key model. On the other hand, the weakness in the key schedule can be applied in the SQUARE and meet-in-the-middle attacks. It can assist to gain free bytes of sub-keys for extending the targeted rounds of attack. Since most current attacks focus on maximizing the number of rounds that can be broken and on minimizing the time and data complexity, these security vulnerabilities caused by key schedules are worthy of further study. There are many modification variants for AES, especially for its key schedule aim to patch the security flaw.

The block cipher AES has a 128-bit state and supports three key sizes: 128, 192 and 256 bits. It is a byte-oriented cipher and has 10 rounds for 128-bit, 12 rounds for 192-bit and 14 rounds for 256-bitkeys. In each round of AES, the internal state can be seen as a 4×4 matrix of bytes, which undergo the following basic transformations:

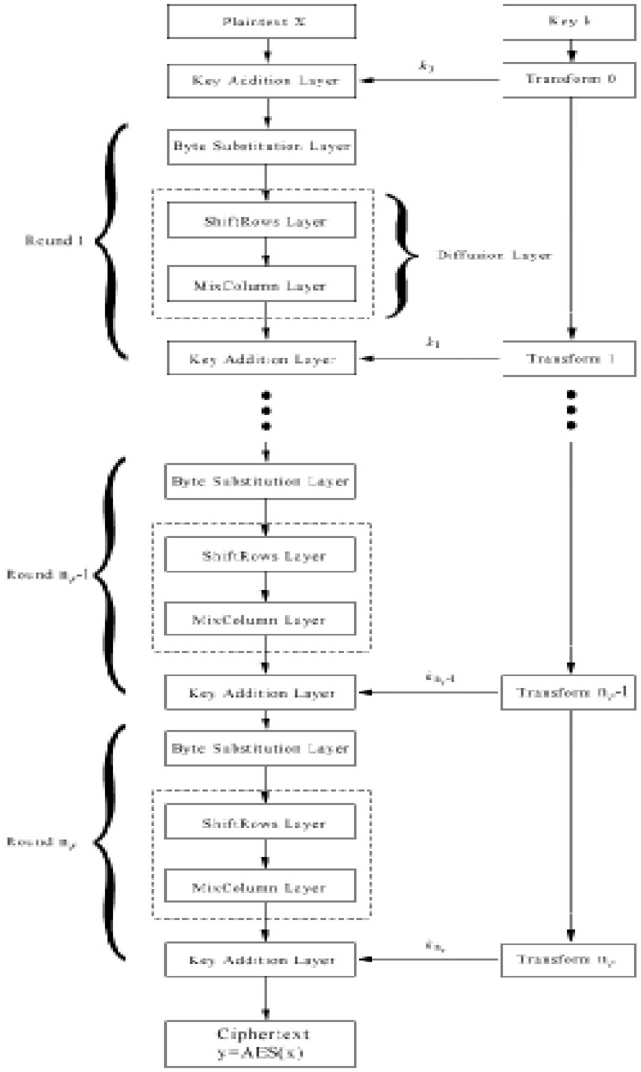

Fig. 2: The encryption of AES

- **Sub bytes:** Byte-wise application of S-boxes, abbreviated as SB (.).
- **Shift rows:** Cyclic shift of each row of the state matrix by some amount, abbreviated as SR (.).
- **Mix columns:** Column-wise matrix multiplication, abbreviated as MC (.).
- **Add round key:** XOR of the sub key to the state, abbreviated as ARK (.).

An additional Add Round Key operation is performed before the first round (the whitening key) and the Mix Columns operation is omitted in the last round.

The key schedule is required to produce 11, 13 or 15 128-bit subkeys from master keys of size 128, 192 or 256 bits respectively.

Each 128-bit subkey contains four words (a word is a 32-bit quantity which is denoted by W [·]). Call the number of rounds Nr and the number of 32-bit words in the master key Nk (e.g., for AES-128, Nr = 10, Nk = 4):

- For i = 0, . . ., Nk-1: W [i] = K [i], where K [·] is the master key.
- For i = Nk, . . . , 4 (Nr + 1):
    - Temp<---- W [I - 1].
    - If i mod Nk == 0: temp <---- SB (RotWord (temp)) ⊕ RCON [i/Nk].
    - If Nk = 8 and i mod 8 = = 4: temp <---- SB (temp).
    - W [i] <---- W [i - Nk] ⊕ temp.

where RCON [·] are round constants and RotWord (·) rotates four bytes by one byte position to the left.

The sub key used in the Add Round Key at the end of round r is denoted by k_r. The whitening key is k_{-1}. Each sub key is represented as a byte matrix of size 4×4

(corresponding to the state matrix) and the j'th byte in the i'th row of the matrix is denoted by $k^r_{i,j}$ (for 0<i, j<4). The "equivalent" key obtained when the Mix Columns and Add Round Key operations are interchanged is denoted by $k'_r = MC^{-1} (k_r)$.
The process of AES encryption is as Fig. 2.

AES is the most widely used block cipher so its security is proved. Even though the term "Standard" in its name only for US government applications, the AES block cipher is also widely used in other industry standards in the word. AES is also used in many systems with high security requirements. These systems include the TLS, Internet security standard IP sec, the IEEE 802.11i, Wi-Fi encryption standard, the secure shell network protocol SSH (Secure Shell), the Skype and so on.

RESEARCH OF ASYMMETRIC ALGORITHM AND RSA

Three MIT professors (Rivest Ronald L, Shamir Adi and Adleman, Leonard M) invented the RSA public-key cryptosystem, which includes encryption and decryption key for two different key cryptosystems. It uses a pair of keys: one called the public key PK, is open for the usage by others. Its role is to encrypt or generate digital signatures. Another key is known as the private key SK for the usage by the user who is confidential. This key is used to decrypt the digital signature of the message. The relationship between the two keys is that, any one of the keyed information can only be decrypted with another key and the decryption key cannot be obtained from the encryption key. Because the public key is as an encryption key and the private key is for decrypting, you can achieve multiple users to encrypt the information. The cipher texts can only be interpreted by a user. Vice versa, you can implement a user to encrypt information with his private key and is interpreted by multiple users. The former is used for the data encrypting, the latter is used for digital signatures.

The so-called asymmetric key cryptography system is to encrypt and decrypt using different key cryptographic techniques. The user has selected a pair of keys: a public key (allows all communication people to know) and a private key. Another security is owned by the user, which is the private key specifically for them. The public key and the private key cannot be launched by another public key encryption. The information can only be decrypted by the private key and vice versa. The communication of asymmetric encryption algorithm is as Fig. 3.

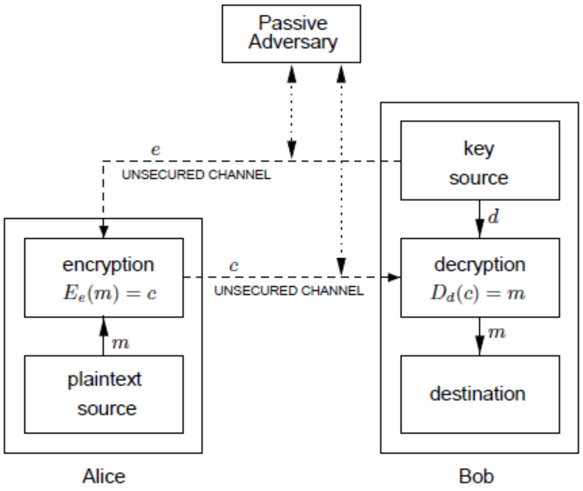

Fig. 3: The communication of asymmetric encryption algorithm

There are several widely used public-key algorithms: RSA public key encryption, knapsack algorithm, ElGamal algorithm, elliptic curve cryptography algorithms.

Similarly, the asymmetric cryptosystem has advantages and disadvantages. With the using of the public key encryption algorithm, communications can be successful in advance without the use of secret passages and complex protocol. Key exchange can establish a secure communication public key encryption channel for implementing digital signature and identity recognized certification.
To sum up, the advantages are as follows:

- The key is easy to manage: the network households simply save your own decryption key, the N users only produce N keys
- Good for key distribution
- Does not require secret channels or complex agreements to send the key and achieve the digital signature

The disadvantage is that the asymmetric key algorithm possesses a slower speed than symmetric key algorithms.

In this study, we use RSA as the required public key algorithm.

A NEW SECURE SCHEME FOR ELECTRONIC COMMERCE

In this section, we study the practical realizations of the 3-round cipher constructed from AES. We combine the usage of asymmetric ciphers and symmetric ciphers,

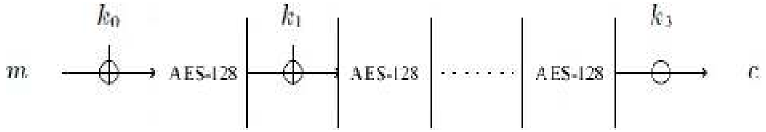

Fig. 4: The structure of our block cipher based on AES-128

as previous work. However, as mentioned above, the block cipher AES which is widely used has been broken theoretically, so here we search for a new and more secure replacement for it. We propose a new cipher proposal based on AES, but has provable security about its effective key length. After using this new block cipher with the asymmetric cipher RSA, instead of the original AES, we obtain a new scheme for electronic commerce that can still run fast, but is safer.

A natural method is to build a cipher in practice following the t-permutation structure. We base the 3 fixed permutations on AES by fixing some keys.

We first discuss this structure. If t = 1, then we construct an Even-Mansour construction (Shimon and Yishay, 1997). The resulted block cipher has a security level which is only $2^{n/2}$ and n is the block size. For AES, the block size is 128 bits, so we can only get 2^{64} effective key bits. So we need to choose t>1. In this context, we choose t = 3 and consider this is enough. We also prove the security when t = 3 in our experiments Section.

AES^3: a block cipher proposal for electronic commerce based on AES: The construction is made up by mixing three AES-128 permutations by randomly choosing three keys. These three keys determined the three permutations. All of these three keys are independent. Denote AES (k) as the AES-128 with a 128-bit key k. Constants are also needed and we choose them randomly in this section:

C1 = 0xd314327543203707344a4093822299f31
C2 = 0xd0082efa98ec4e6c89467576576585a308
C3 = 0xd00345093485eabcd94673450998345ede

The four key needed in the new block cipher are k0, k1, k2, k3. The structure of the new structure for our block cipher is as Fig. 4.

AES3 [k0, k1, k2, k3] (x): = AES [C3] (AES [c2] (AES [c1] (m⊕k0) ⊕k1) ⊕k2) ⊕k3.

Performance: AES^3 can be implemented very effectively in hardware and software on the computer processors with general purpose or ordinary hardware. We can pre-compute the keys for the three AES transformations.

Table 1: The comparison of the speed of our block cipher proposal with AES-128

	Intel XEON, X5670	Intel core i7, 640M
ECB, AES3	2.11	2.14
CTR, AES3	2.34	2.23
ECB, AES-128	1.76	1.89
CTR, AES-128	1.87	1.98
CTR, AES-128	7.35	7.68
CTR, AES-128	15.98	16.17

The three AES keys C1, C2 and C3 are fixed, so there is no need to carry the key schedule of AES. This ensures high key agility of AES^3.

On the architecture generation of Intel general-purpose processors, AES^3 can be implemented using the AES-NI instruction set. As the AES round instructions are pipelined, we completely pipeline by processing five independent plaintext blocks in parallel. The basic ECB mode and CTR mode are achieved easily. The efficiency of these implementations on latest processors proved is and compared with the other two traditional AES-128 implementations: (i.e., without AES-NI instructions), the Open SSL 1.0.0e implementation based on lookup tables and the bitsliced (Emilia and Peter, 2009) implementation. All numbers are given in Cycles per Byte (CPB) (Table 1).

Table 1 shows that our improved AES^3 still has a high speed for implementation. This is very important in the actual application of electronic commerce. The electronic commerce needs the data being transmitted as fast as possible at every step.

OUR EXPERIMENTS

In this section, in order to show the security of our scheme, we carry some experiments. We use the property of unpredictability to measure the security margin, which is a basic property in the cryptanalysis. We take XML data files that are generated with our scheme and separate them into 600 1000-bit sequences and 500 1500-bit sequences. We also use the AES^3 in the digital signature and compute the results as follows. Once observed some non-random regularity in these sequences, our scheme may face great risks and is regarded as dangerous. We test the following statistics on our data.

p-value is a measurement for above statistics and it is a probability value with range of [0, .., 1]. The larger

Table 2: The results of the digital signature based on our block cipher proposal

Index of texts	p-value of XML data files	p-value of digital signature
1	0.897	0.802
2	0.843	0.83d
3	0.787	0.735
4	0.776	0.735
5	0.816	0.823
6	0.903	0.687
7	0.649	0.593
8	0.867	0.895
9	0.750	0.732
10	0.876	0.833
11	0.686	0.625
12	0.603	0.611
13	0.677	0.604
14	0.623	0.598
15	0.668	0.621
16	0.754	0.801

the p-value is, the safer our scheme is. A small p-value means that the probability of occur of the sequences is small, which shows a non-random property. The most widely used randomness tests are in the suite proposed by NIST in 2000. In this suite, there are 16 statistical tests and each of them focuses on a distinct pattern for the sequences, which are the signature in our context. The larger the p-value and the safer the digital signature are shown in Table 2.

CONCLUSION

Electronic Commerce (EC) has allowed organizations to enhance their economic growth, reduce the barriers of market entry, improve the efficiency, keep the inventories lean and reduce the costs and so on. In fact, many customers have found the power of using the Internet: convenience, more choice for products and services, vast amounts of information and time saving. They are not going to let a poor economy stop them from taking advantages of the electronic commerce. The large demands of electronic commerce lead to a huge requirement for the security. With the rapid growth of the computer and network communication, these requirements are becoming higher and higher. We need to focus on more security issues in the applications of electronic commerce. In this study, we have investigated the latest results of the security algorithms that are used in electronic commerce. We study the disadvantages and advantages of both the asymmetric algorithms and the symmetric algorithms. We propose a more secure usage on them. Then we provide a new scheme that combines the improved symmetric algorithm AES and asymmetric algorithm RSA. Sound reasons are given to explain why we choose this scheme. Finally, we prove the security of our scheme by showing the experimental results.

ACKNOWLEDGMENT

The studies was supported by the Education Department of Hubei Province (B20092305); Science Foundation of the Education Department of Hubei Province (D20111802).

REFERENCES

Bogdanov, A., D. Khovratovich and C. Rechberger, 2011. Biclique cryptanalysis of the full AES. Lect. Notes Comput. Sci., 7073: 344-371.

Daemen, J. and V. Rijmen, 1998. AES proposal: Rijndael. Proceeding of the 1st AES Candidate Conference, pp: 1-37.

Emilia, K. and S. Peter, 2009. Faster and timing-attack resistant AES-GCM. Lect. Notes Comput. Sci., 5747: 1-17.

Jiqiang, L., 2011. The (related-key) impossible boomerang attack and its application to the AES block cipher. Des. Code Cryptogr., 60(2): 123-143.

Khiabani, Y.S. and W. Shuangqing, 2011. Creation of degraded wiretap channel through deliberate noise in block ciphered systems. Proceeding of the IEEE Topic(s): Communication, Networking and Broadcasting, GLOBECOM Workshops (GC Wkshps), pp: 893-897.

Mitsuru, M., 1993. Linear cryptanalysis method for DES cipher. Lect. Notes Comput. Sci., 765: 386-397.

Shimon, E. and M. Yishay, 1997. A construction of a cipher from a single pseudorandom permutation. J. Cryptol., 10(3): 151-162.

Wang, X., H. Yu and Y.L. Yin, 2005a. Efficient collision search attacks on SHA-0. Adv. C.-Crypto., 3621: 1-16.

Wang, X., X. Lai, D. Feng, H. Chen and X. Yu, 2005b. Cryptanalysis of the hash functions MD4 and RIPEMD. EUROCRYPT, 3494: 1-18.

Yongzhuang, W., L. Jiqiang and H. Yupu, 2011. Meet-in-the-middle attack on 8 rounds of the AES block cipher under 192 key bits. Inform. Sec. Practice Exp., LNCS, 6672: 222-232.