Virtual-optical information security system based on public key infrastructure

Xiang Peng *a,b, Peng Zhang **b, Lilong Cai c, Hanben Niu a

a. Institute of Optoelectronics, Shenzhen University, Key laboratory of Optoelectronic Devices and Systems of Education Ministry, 518060 Shenzhen, China
b. National Laboratory of Precision Measurement Technology and Instrumentation, Tianjin University, 300072 Tianjin, China
c. Department of Mechanical Engineering, Hong Kong University of Science and Technology Clear Water Bay Kowloon, HKSAR, China

ABSTRACT

A virtual-optical based encryption model with the aid of public key infrastructure (PKI) is presented in this paper. The proposed model employs a hybrid architecture in which our previously published encryption method based on virtual-optics scheme (VOS) can be used to encipher and decipher data while an asymmetric algorithm, for example RSA, is applied for enciphering and deciphering the session key(s). The whole information security model is run under the framework of international standard ITU-T X.509 PKI, which is on basis of public-key cryptography and digital signatures. This PKI-based VOS security approach has additional features like confidentiality, authentication, and integrity for the purpose of data encryption under the environment of network. Numerical experiments prove the effectiveness of the method. The security of proposed model is briefly analyzed by examining some possible attacks from the viewpoint of a cryptanalysis.

Keywords: virtual-optics, information security, public key infrastructure, asymmetric algorithm, digital signatures

1. INTRODUCTION

Information security is a fast growing research subject that has drawn increasing attention from both academic and industrial circles as it covers a great number of application areas in the field of information technology to prevent huge economic losses. Recently, a number of optical methods have been proposed for the purpose of information hiding and data security, because optical information processing techniques have obvious advantages such as inherent parallel processing capability, more degrees of freedom (e.g. amplitude, phase, polarization, wavelength) for encryption and decryption, and high-level data security 1-5. However, most published works on optical encryption techniques belong to symmetric cipher techniques from the point of view of cryptosystem, which means that the processes of both encryption and decryption use identical key. In such a cryptosystem, senders must still address how to safely deliver the secret key to recipients in addition to algorithm strength and length of key, which is not trivial task in an open network environment 6. Besides, in the symmetric cryptosystem, the issues of reliable key distribution, key delivery, and key management have not been addressed properly. With these problems existed, it is difficult for current optical encryption techniques to incorporate with international standard or protocol for the information security, so that it could not be appropriate for practical applications.

Recently, Lin et al. 7 used public key algorithm together with the scheme of double-random-phase encoding 1 to construct a public-key-based optical image cryptosystem in which the symmetric keys of encryption could be safely transferred. However, they did not provide a reliable and practical means for user identity authentication and integrity verification. So it can be weak to “forgery attacks” 6.

* xpeng@szu.edu.cn; phone +86 755 26538548; fax +86 755 26538580; http://opto.szu.edu.cn/cn/Member/PengX.htm
** pengzhang@tju.edu.cn; phone +86 22 87401745; http://www.tju.edu.cn
In this paper we present a virtual-optical based encryption model with the aid of public-key-infrastructure (PKI). The proposed model employs a hybrid architecture in which our previously published encryption algorithm based on virtual-optics scheme (VOS) can be used to encipher and decipher data while an asymmetric algorithm, for example RSA, is applied for enciphering and deciphering the session key(s). For an asymmetric system, given an encryption key, it is computationally infeasible to determine the decryption key and vice versa. The whole information security model is run under the framework of international standard ITU-T X.509 PKI, which is on basis of public-key cryptography and digital signatures. This PKI-based VOS security approach has additional features like confidentiality, authentication, and integrity for the purpose of data encryption under the environment of network.

2. BACKGROUND OF VIRTUAL-OPTICS SCHEME

Our previously published encryption method based on VOS is briefly reviewed in this section. As show in Fig. 1, suppose that both object-plane (host data sheet) and the random mask (RM) are “illuminated” with the same coherent light wave with virtual wavelength $\lambda^s$.

In the process of encryption, we take the Discrete Fresnel diffraction (DFD) transform for host data sheet (denoted by $U_o$) and random mask (denoted by $U_M$) through the propagating distance $d_o$ and $d (d = d_1 + d_2)$, respectively. The DFD patterns of host data sheet and random mask will interfere each other at front plane of imaging lens to form an interferogram. The interferogram is further converted by lens transmission function and forwarded to back plane of the lens. The complex amplitude distribution at back plane of imaging lens (denoted by $U_{l2}$) is taken as enciphered data, and it will be sent through a communication channel as an ordinary electronic file. The encryption process can describe by following equation:

$$U_{l2}(m,n) = \{DFD[U_o(k,l);\lambda,d_o] + DFD[U_M(k,l);\lambda,d]\} \times t(m,n;f)$$  \hspace{1cm} (1)
We have demonstrated\(^8\) that parameters \(d_o, d, f\) and \(\lambda\) together with the random mask offer a huge space for the key designs in the process of data encryption.

At the end of receiver, the decryption process can be achieved via following steps: (1) taking DFD transformation of the informed RM (denoted by \(U_M'\)) through a diffraction distance \(d\), and multiplying by transmission function of imaging lens to obtain the complex amplitude distribution at the back plane of the lens with given focal length \(f\); (2) subtracting this pattern from enciphered data, the result is denoted by \(U'\); (3) taking another DFD transformation to \(U'\) through a propagating distance \(d\), which can be deduced from \(d_o\) and \(f\) to obtain the image of host information sheet and therefore recover the hidden information sheet. The decryption process can be described by following equation

\[
U'(m, n) = DFD[U'(k, l); \lambda, d_1(d_o, f)]
\]

Where

\[
U'(m, n) = U_{I2}(m, n) - DFD[U_M'(k, l); \lambda, d] \times t(m, n; f)
\]

It can be clearly seen from decryption process that if one wishes to completely recover the hidden information sheet, he has to know four parameters, namely \(d_o, f, d, \lambda\), except for the RM.

From the encryption and decryption procedures, we can see that the Virtual-Optical encryption algorithm uses the same key(s), such as \(d_o, f, d, \lambda\), RM, in the sender and receiver. So this approach is still categorized as symmetric key cryptosystem.

3. PKI-BASED VOS INFORMATION SECURITY MODEL

3.1. Hybrid cryptosystem based on VOS

Although asymmetric key cryptography seems ideal for the secure communications, it is much slower than symmetric systems, making it unsuitable for transferring large documents. The fact that symmetric keys are unmanageable, and that asymmetric cryptography is computationally very intensive produces a dilemma. Both technologies have deficiencies that limit their practical use in current optical encryption systems. In order to achieve a functional system, we present a hybrid approach, which combines the advantages of both kinds of cryptographic techniques in order to overcome the limitations for each of them.

The proposed cryptosystem employs a hybrid architecture in which our previously published encryption method based on VOS\(^{8-9}\) can be used to encipher and decipher data while an asymmetric algorithm is applied for enciphering and deciphering the session key(s). Firstly, the symmetric encryption keys (or session keys) derived from Virtual-Optics are randomly generated for each data encrypting operation. Then the recipient’s public key is used to encrypt the session keys. When receiving the data, the recipient decrypts the session keys using his/her corresponding private key. Once the session keys are extracted they are then used to decrypt the host data.

3.2. System architecture design
Virtual optical encryption algorithm is efficient to deal with the encryption of host data whilst asymmetric cryptography is good at solving the problems of key distribution. The proposed framework described in Section 3.1 seems to be fine as it could be able to fit the optical encryption concepts into modern information security system seamlessly. However, one issue remained is how to distribute the public keys with a proper way. Any illegal user can forge a public announcement and pretends to be a legal user A, and send a public key to another participant. Thus, the forger is able to obtain all encrypted messages intended for A, To avoid such an accident, it must make sure that only legal user(s) can obtain the given public key. The process that associates an individual with a particular public key is referred to as “identity authentication” or “certification”, which is the fundamental issue of all PKIs. The CA scheme described in the ITU-T X.509 provides an international standard for certification. The CA is an entity that issues and revokes the certificates. CA will create a digital signature to the information sheet about the user and corresponding public key; then issues certificates by binding the identity of a user or system to his public key with the digital signature. These certificates are placed in an open directory by the CA. Anyone could look up the directory and get the digital certificate of the entity with which he will communicate. Using the CA’s public key, he could verify the validity of digital certificate, and thus the validity of public key included in the certificate. The user’s identity is indicated in the digital certificate, which is unique to the particular user. CA is in charge of issuing and managing digital certificates. Before creating a session (secure communication), users should verify the identity of each other via the digital certificates and CA. Thus, the content and authenticity of the communication are guaranteed. The process of issuing digital certificates will be described in detail in Section 3.3. The functional blocks of information security framework based on Virtual-Optics and PKI are shown in Fig.2.

As shown in Fig.2, the secure communication process under the framework of our proposed model can be briefly summarized as the following major steps:

On the side of sender:
1. The symmetric encryption keys or session keys derived from Virtual-Optics are randomly generated for each data encrypting operation.

\[
K_{\text{session}} = \text{RNG}(d_0, d, f, \lambda, \text{RM} \ || \ \text{Seed})
\]

where \( \text{RNG}(\cdot) \) represents a pseudo random number generator, \( d_0 \) and \( d \) denote the diffraction distance respectively, \( f \) denotes the focal length of the imaging lens, \( \lambda \) denotes the virtual wavelength, RM is the random mask. It is worth pointing out that the physical parameter such as the virtual-wavelength could be secretly selected from a huge numerical range instead of one coming from a physically existing laser source.

2. Sender encrypts the plaintext with the session keys to obtain the ciphertext. This process can be described by the Eq. (1).

3. Sender verifies receiver’s digital certificate signed by CA using the public key \( PK_{\text{CA}} \) also issued by CA. Thus, the validity of the receiver’s public key \( PK_R \) included in this digital certificate is also verified.

\[
PK_R \leftarrow \text{Authentication (Certificate \ || \ PK_{\text{CA}})}
\]

where Authentication (\( \cdot \)) represents the process of digital certificate verification. More details about this process will be given in Section 3.4.

4. The session keys are encrypted with the receiver's public key \( PK_R \):

\[
c = E_{PK_R}(K_{\text{session}})
\]

where \( E_{PK_R}(\cdot) \) represents an asymmetric encryption function (such as RSA) and \( c \) denotes the result of the asymmetric encryption.

5. The ciphertext and the encrypted session keys are sent to the receiver together through a communication channel as an ordinary electronic file. This becomes the "Digital Envelope.” In fact, the digital envelope is a code within a code. The public key method is used to exchange the secret key, and the secret key is used to encrypt and decrypt the message.

**On the side of receiver:**

1. Receiver decrypts the session keys using his corresponding private key \( SK_R \):

\[
K_{\text{session}} = D_{SK_R}(c)
\]

where \( D_{SK_R}(\cdot) \) represents an asymmetric encryption function (such as RSA). Because the private key \( SK_R \) is known ONLY to the key holder (that is, receiver), attacker can’t acquire the correct session keys \( K_{\text{session}} \).

2. Once the correct session keys \( K_{\text{session}} \) are obtained, the receiver then know the correct parameters utilized in the encryption process, such as \( d_0, d, f, \lambda \) and the random mask RM.

3. Receiver decrypts the message with correct parameters according to Eq. (2) and Eq. (3).

4. The plaintext is obtained, and then a successful secure communication is completed. The message is secure because it is encrypted using a symmetric session key that only the recipient and sender know.

### 3.3. Signing the receiver’s digital certificate

A content of digital certificate contains pieces of information, such as indicated the user name, public key for the user, and a digital signature of CA, etc. Trusted Certification Authority (CA) produces a digital signature with its private key. Practically, A digital certificate can have a number of different formats. For example, X.509 certificate is a very common certificate format that complies with the ITU-T X.509 international standard.

The CA signs the receiver’s digital certificate in a two-step process. Firstly, the message data \( M \) (including public key for the receiver) is compressed using a one-way Hash function \( H \), which transforms the information sheet with arbitrary length into a string of fixed length, leading to a so-called message digest \( H(M) \). Then the message digest is
encrypted with the CA’s private key $SK_{CA}$. The encrypted message digest becomes the digital signature $S$ that forms one part of the digital certificate. Because the digital signature is unforgeable, the certificate can be stored in an open directory. From the certificate, the sender can verify the recipient’s identity and recover his or her public key.

Aforementioned hash function can be the MD5 message-digest algorithm\textsuperscript{11} developed by Ron Rivest at MIT or the SHA-1 hash algorithm\textsuperscript{12} developed by the National Institute of Standards and Technology (NIST). They are both widely used secure hash algorithms.

The hash functions can transform a string of characters into a usually shorter fixed-length value or key that represents the original string. A slight change in the original file will result in a totally different hashed file. The fixed-length value, called message digest, can be encrypted and then used as a digital signature. For different message, one will have different digital signature that is authentic, not reusable, unforgeable, unalterable, and cannot be repudiated. Digital signature function can also be the RSA Public Key digital signature algorithm, which is the easiest implementation and most widely used approach\textsuperscript{6}.

### 3.4. Confirming receiver’s public key by verifying his digital certificate

In our proposed model, the integrity of the receiver’s public key and the identity of the certificate holder should be verified before the real secure communication start. As shown in Fig. 3, with the public key $PK_{CA}$ given by CA the sender needs to firstly extract the message digest via decrypting digital signature $S$. The digital signature has been included in the receiver’s digital certificate. The sender also needs to re-compute the message digest from the received message data $M$ with the same hash function $H$. If the decrypted message digest matches the calculated message digest, the message is authenticated, verifying that the data has never been altered. Thus, the validity of the receiver’s public key $PK_R$ included in the digital certificate is also verified. Otherwise, the authentication fails and the signature cannot be accepted.

![Fig. 3 The procedure of verifying a digital certificate](image-url)
4. SECURITY ANALYSIS OF PROPOSED MODEL

In this section, the security of proposed model is briefly analyzed by examining some possible attacks from the viewpoint of a cryptanalysis.

4.1. Ciphertext-only attack

In such an attack, attackers are assumed to have only the ciphertext and do not have the symmetric encryption keys (or session keys). Without the session keys, that is without the correct parameters $d_o,d,f,\lambda$, RM utilized in the encryption process, attackers can’t recover the plaintext. Moreover, we have demonstrated that these parameters offer a huge space for the key designs in the process of Virtual-Optical data encryption. So attackers try to guess the session keys using a brute force search is computationally infeasible.

4.2. Known-plaintext and chosen-plaintext attacks

In a “known-plaintext” attack, attackers have obtained plaintext-ciphertext pairs. In a “chosen plaintext” attack, attackers can submit selected plaintext to encrypt and gain access to the resulting ciphertext. In these two attacks, attackers can analyze the encrypted message to infer the multidimensional data encryption keys and then are able to decrypt subsequent message correctly if the sender continues to encrypt the plaintext using the same session keys. Crypto-system, which resists ciphertext-only attack, might still be susceptible to these two attacks.

But in our proposed system, the multidimensional data encryption keys (or session keys) are changed periodically to enhance the security of communication. The diffraction distance $d_o$ and $d$, focal length of the imaging lens $f$, virtual wavelength $\lambda$, and random mask RM derived from Virtual-Optics are randomly generated when secure communication is established and is destroyed when no longer needed, which makes the known-plaintext or chosen plaintext attack very difficult.

4.3. Modification

The message integrity could be retained in our approach. Suppose an attack in which the public key is altered by modifying the digital certificate. Because the digital certificate has been digitally signed by CA, the sender could easily find out that the public key included in the digital certificate is altered by using CA’s public key. The attack fails.

4.4. Forgery attacks

Under the network environment, users could not “see” each other and get other entities’ public keys. Attacker could pretend to be user A and send a public key to another participant or broadcast such a public key. Until user A discovers the forgery and alerts other participants, the forger would be able to read all encrypted messages by pretending to be a legal user A. But in our approach, the Certification Authority (CA) is involved in the operation to help us verifying the user’s public key. So the forgery mentioned above should not be successful since identities of all users involved must be authenticated.

5. CONCLUSION

In conclusion, we have introduced a virtual-optical based encryption model with the aid of public key infrastructure (PKI). The proposed model employs a hybrid architecture in which a symmetric encryption method based on VOS is used to encipher and decipher data while an asymmetric algorithm is applied for enciphering and deciphering the session keys (encryption keys). The whole information security model is run under the framework of international...
standard ITU-T X.509 PKI, which is on basis of public-key cryptography and digital signatures. In addition, the security of proposed model is briefly analyzed by examining some possible attacks from the viewpoint of a cryptanalysis.

ACKNOWLEDGEMENT

This project is supported by National Science Foundation of China (NSFC) through the research project No. 60472107, and Research Grants Council (RGC) of HK SAR. The sponsorship from the NLPR, Chinese Academy of Science (CAS) through an Opening Research Project is also greatly acknowledged.

REFERENCES