New Public-Key Cryptosystem Based on Two-Dimension DLP

Xiaoqiang Zhang
State Key Lab of Software Development Environment, Beihang University, Beijing, China
Email: grayqiang@163.com

Guiliang Zhu, Weiping Wang and Mengmeng Wang
North China University of Water Conservancy and Electric Power, Zhengzhou, China
Email: zgg500@126.com; wangweiping888@qq.com; 295612840@qq.com

Shilong Ma
State Key Lab of Software Development Environment, Beihang University, Beijing, China
Email: slma@nlsde.buaa.edu.cn

***Abstract*—The asymmetric cryptosystem plays an important role in the cryptology nowadays. It is widely used in the fields of data encryption, digital watermarking, digital signature, secure network protocol, etc. However, with the improvement of computing capability, longer and longer the key length is required to ensure the security of interaction information. To shorten the key length and improve the encryption efficiency, by defining the two-dimension discrete logarithm problem (DLP), a new public-key cryptosystem is proposed. This new cryptosystem generalizes the public-key cryptosystem from one dimension to two dimensions. The core algorithms of the proposed cryptosystem are also designed, including the fast algorithm, computing the inverse matrix modulo p and finding the period. To verify the correctness and rationality of the new cryptosystem, two examples are carried out. Meanwhile, the efficiency and security are analyzed in detail. Experimental results and theoretical analyses show that the new cryptosystem possesses the advantages of the outstanding robustness, short key length, high security and encrypting many data once.**

***Index Terms*—asymmetric cryptosystem, discrete logarithm problem (DLP), two dimensions, RSA, ECC (elliptic curve cryptosystem)**

I. INTRODUCTION

The cryptosystems can be classified as the symmetrical cryptosystem and the asymmetrical cryptosystem (also named as the public-key cryptosystem) by the characteristics of the key. For the symmetrical cryptosystem, $n(n-1)/2$ keys are required to satisfy the secure communication among n users over the Internet. The key distribution and management become very difficult when n is a very large number. However, the asymmetrical cryptosystem just requires $2n$ keys, whose key distribution and management are much easier. Meanwhile, the asymmetrical cryptosystem cannot only use for data encryption [1-3], but also for digital signature and authentication [4-6].

As a landmark of the cryptology development, W. Diffie and M. E. Hellman proposed the concept of public-key cryptosystem in 1976 [7]. Afterwards many public-key cryptosystems are proposed. Experts in cryptology select three types of asymmetrical cryptosystem, which are regarded as the secure and efficient cryptosystems. The detailed description is as follows.

- The cryptosystem based on the integer factorization problem (IFP): Its representative is RSA (Rivest, Shamir, Adleman), which was proposed in 1977 [8]. The advantages of RSA are the simple principle and easy application. RSA cryptosystem is designed based on two big prime numbers p and q instead of a two-dimension matrix. Meanwhile, the plaintext M is segmented to several data blocks m_i, $i = 1, 2, 3, \cdots$ in advance, and each data block m_i can correspond a decimal number n_i. RSA can only encrypt the number n_i instead of a two-dimension plaintext matrix during an encryption process [9]. However, with the improvement of the integer factorization algorithm, we need to continuously lengthen the key length of RSA to ensure the security of the cipher text. 768 bits RSA is unsecure at present, and experts suggest applying 1024 bits RSA to ensure the 10-year security. To ensure the 20-year security, we are required to choose 2048 bits RSA. Although the extending of the key length can enhance the security of RSA cryptosystem, the encryption speed reduces sharply and the application becomes very difficult.
- The cryptosystem based on the discrete logarithm problem (DLP): Its representative is DSA (digital

Manuscript received January 30, 2011; revised June 25, 2011; accepted June 26, 2011.
Corresponding author: Xiaoqiang Zhang.

doi:10.4304/jcp.7.1.169-178

signature algorithm), which was proposed by the National Institute of Standards and Technology (NIST) in August 1991. It is a United States Federal Government standard for digital signatures.

- The cryptosystem based on the elliptic curve discrete logarithm problem (ECDLP): Its representative is ECC (elliptic curve cryptosystem). Koblitz and Miller proposed ECC in 1985 [10, 11]. The ElGamal scheme of ECC is designed based on a basic point of the elliptic curve instead of a two-dimension matrix. Meanwhile, the plaintext M is encoded to several corresponding points of the elliptic curve in advance, and then ECC can only encrypt one of these points instead of a two-dimension plaintext matrix during an encryption process [12]. ECC possesses the advantages of the short key length, fast speed, etc [13]. There is not an effectively deciphered method at present [15].

With the improvement of computing capability, the key length becomes longer and longer to maintain the security of interaction information. The increasing of the key length makes the encryption efficiency low. Meanwhile, current asymmetric cryptosystems are one dimension, which can only encrypt a datum once. To improve the encryption efficiency, it is reasonable to generalize the public-key cryptosystem from one dimension to two dimensions, and even high dimensions. Therefore, by defining two-dimension DLP, a new public-key cryptosystem is proposed in this paper. This cryptosystem generalizes the public-key cryptosystem from one dimension to two dimensions.

The rest of the paper is organized as follows. We generalize the definition of DLP from one dimension to two dimensions in Section II. Section III designs the new cryptosystem based on the two-dimension DLP. The fast algorithm for the proposed cryptosystem, the algorithm of computing the inverse matrix modulo p and the algorithm of finding the period are designed in Section IV. To verify the correctness and rationality of the new cryptosystem, two examples are carried out respectively in Sections V and VI. The efficiency analysis of the new cryptosystem is given in Section VII. The security analysis of the new cryptosystem is discussed in Section VIII. Section IX concludes the paper.

II. DLP

Solving DLP is a difficult mathematic problem at present, which plays an important role in cryptology. DLP is described as follows.

Let G be an Abelian group comprised of numbers. $\langle\alpha\rangle$ denotes a subgroup of G generated by $\alpha \bmod p$, where $p>3$ and p is a prime. Supposing $\beta \in \langle\alpha\rangle$, the discrete logarithm $\log_\alpha \beta$ is the smallest non-negative integer x such that $\alpha^x \bmod p = \beta$. DLP is computing $x = \log_\alpha \beta$ under the premise of given α and β [14]. For easy discussion, we call this problem as one-dimension DLP.

The matrix possesses more elements and complexer construction than a number. As an extension, we define the two-dimension DLP as follows.

Let G be an Abelian group comprised of matrixes. $\langle A\rangle$ denotes the subgroup of G generated by a matrix $A \bmod p$, where $p>3$ and p is a prime. Supposing $B \in \langle A\rangle$, the discrete logarithm is the smallest non-negative integer x such that $A^x \bmod p = B$. The two-dimension DLP is computing $x = \log_A B$ under the premise of given A and B. Notice that $\log_A B$ is just a denotation to unify the form.

III. NEW PUBLIC-KEY CRYPTOSYSTEM

A new public-key cryptosystem based on the two-dimension DLP is designed by using slightly altered Elgamal cryptosystem [15]. Supposing the following scenario, Alice is a sender and Bob is a receptionist. The detailed steps of this new cryptosystem are described as follows.

A. Bob's key-generating steps

Bob needs to generate his public key and private key before decrypting Alice's information. The detailed steps are as follows.

- Choose a matrix $A_{n\times n}$ comprised of the elements from the set $Z_p = \{0,1,2,\cdots,p-1\}$, where $|A| \neq 0$, A cannot be the identity matrix I, p is a prime or $p = 2^m$, and $\gcd(|A|, p) = 1$.
- Compute the period T of the generator $A \bmod p$, and then he can obtain a cyclic group $G_p = \{I, A, A^2, A^3, \cdots, A^{T-1}\}$.
- Randomly select an integer $d \in \{1,2,\cdots,T-1\}$ as his private key and calculate the matrix $Q = A^d \bmod p$.
- Publish the public key $[A, T, p, Q]$.

B. Alice's encryption steps

Alice performs the following steps to encrypt the plaintext.

- Acquire Bob's public key $[A, T, p, Q]$.
- After randomly selecting an integer $u \in \{1,2,\cdots, T-1\}$, Alice calculates the matrixes $C = A^u \bmod p$ and $D = Q^u \bmod p$ with Bob's public key.
- Let a matrix $M_{n\times n}$ be the plaintext, whose elements are from the set Z_p. Calculate the cipher text matrix $E = (D \times M) \bmod p$.
- Send the encrypted data $[C, E]$ to Bob.

C. Bob's decryption steps

Bob performs the following steps after receiving Alice's encrypted data $[C, E]$.

- Calculate the matrix $D = C^d \bmod p$ with his private key d. $D = Q^u = (A^d)^u = (A^u)^d = C^d \bmod p$.
- Compute the inverse matrix of D with the equation $(D \times D_p^{-1}) \bmod p = I$, where I is the identity matrix.
- Bob can recover the plaintext M by calculating $M = (D^{-1} \times E) \bmod p$.

IV. ALGORITHMS

A. Fast algorithm

$A^e \bmod p$ is the core operation for the proposed cryptosystem. To improve the encryption efficiency, the square-multiply method for numbers is generalized to matrixes.

The square-multiply method is one of the rapidest methods of computing modular exponentiation [16-19]. The algorithm idea derives from "QinJiuShao" algorithm, which was proposed in Song Dynasty of China [16]. To accelerate the computing, the square-multiply method is used in RSA [16, 18] and ECC [20, 21] at present.

The principle of the square-multiply method is converting the exponent into its binary expression at first. According to the binary expression, the result can be obtained conveniently by changing the expression of modular exponentiation.

E.g., first, convert the exponent e into a binary expression $(e_r, e_{r-1}, \cdots, e_1, e_0)_B$ to compute $a^e \bmod p$, where $e_r = 1$, $e_i \in \{0,1\}$, $i = r-1, \cdots, 1, 0$ and $r = \lfloor \log_2 a \rfloor$. Second, the expression of $a^e \bmod p$ is changed by using Equation (1), and then we can compute the result of $a^e \bmod p$ rapidly.

$$a^e \bmod p = a^{e_r \times 2^r + \cdots + e_1 \times 2^1 + e_0 \times 2^0} \bmod p = a^{e_r \times 2^r} \times \cdots \times a^{e_1 \times 2^1} \times a^{e_0 \times 2^0} \bmod p = ((((\cdots (a^{e_r})^2 \bmod p \times \cdots \bmod p)^2 \times a^{e_1}) \bmod p)^2 \times a^{e_0}) \bmod p. \quad (1)$$

The computing complexity of the square-multiply method is due to the length of the binary expression and the number of "1" in the binary expression.

Similarly, if the number a is substituted for a matrix A, Equation (1) can be rewritten as follows.

$$A^e \bmod p = A^{e_r \times 2^r + \cdots + e_1 \times 2^1 + e_0 \times 2^0} \bmod p = A^{e_r \times 2^r} \times \cdots \times A^{e_1 \times 2^1} \times A^{e_0 \times 2^0} \bmod p = ((((\cdots (A^{e_r})^2 \bmod p \times \cdots \bmod p)^2 \times A^{e_1}) \bmod p)^2 \times A^{e_0}) \bmod p. \quad (2)$$

Therefore, we can rapidly compute $A^e \bmod p$ with the square-multiply method.

B. How to compute the inverse matrix modulo p

The inverse matrix modulo p of the square matrix A is the matrix A_p^{-1} satisfying $(A \times A_p^{-1}) \bmod p = I$, where I is the identity matrix. Meanwhile, A and A_p^{-1} are made up of the elements from the set Z_p. Notice that only if $\gcd(|A|, p) \neq 1$, A_p^{-1} is existing. The process of computing the inverse matrix modulo p is as follows.

- According to $\gcd(|A|, p) = 1$, judge whether A_p^{-1} exist or not. If $\gcd(|A|, p) = 1$, A_p^{-1} exist. Otherwise, A_p^{-1} does not exist.
- If A_p^{-1} exist, compute $|A|$. Otherwise, end.
- Find $i \in Z_p$ satisfying $(|A| \times i) \bmod p = 1$.
- Compute $A_p^{-1} = (i \times |A| \times A^{-1}) \bmod p$, where A^{-1} is the inverse matrix in general.

The Matlab code for computing A_p^{-1} is given as follows.

```
function inverse=invmod(A, p)
%Compute the inverse matrix modulo p of the square matrix A.
%A and its inverse matrix modulo p are made up of the elements from the set Zp={0, 1, 2, ... , p-1}.
%Check input
[row,col]=size(A);
if row~=col
   error('The first parameter must be a square matrix.');
end
det_A=det(A);
%Judge whether the inverse matrix modulo p exist
if gcd(det_A, p)~=1
   fprintf('The inverse matrix modulo %d does not exist.\n', p);
   return
end
%Compute the inverse matrix modulo p
for i=1:p
   if mod(mod(det_A,p)*i, p)==1
      inv_det_A=i;
   end
end
inverse=mod(round(inv_det_A*det_A*inv(A)),p);
```

C. How to find the period T

Taking a square matrix $A_{n \times n}$ as the generator, a cyclic group $G_p = \{I, A, A^2, A^3, \cdots, A^{T-1}\}$ can be obtained, where p is a prime or $p = 2^m$. To find the period T, we design the steps of the algorithm as follows.

- Compute the elements in the first column of $B(:,1) = A \times A(:,1)$.
- Compute $B(:,1) = A \times B(:,1)$ repeatedly, until $B(1,1) = I(1,1)$, where I is the identity matrix.
- Supposing the times of repeated multiplying A is i now, we compute $C = A^i \bmod p$ with the fast algorithm offered in Section IV(A).
- Judge whether $C == I$ or not. If C is equal to I, then $T = i$; else go to Step 2.

The pseudocode for computing the period T is as follows.

```
i=1; B=A; C=A;
While C==I //I is the identity matrix.
{   While B(1, 1)== I(1, 1) //Only judge the first element.
{       B(:, 1)=(A*B(:, 1)) mod p; //Only compute elements in the first column.
i=i+1;
}
C=A^i mod p; //compute A^i with the fast algorithm offered in Section IV(A).
}
T = i;
```

V. A SMALL EXAMPLE

To verify the correctness and rationality of the proposed cryptosystem, a small example is carried out with a matrix $A_{3\times3}$. The result indicates that Bob can recover successfully the plaintext with the new cryptosystem. The detailed description is given as follows.

A. Bob's key-generating steps

- Choose the matrix A and the prime $p = 199867$.

$$A = \begin{bmatrix} 35229 & 81087 & 186969 \\ 183258 & 81999 & 178611 \\ 11570 & 70526 & 162525 \end{bmatrix}.$$

- Compute the period $T = 36987216$ of $A \bmod 199867$.
- Randomly choose the private key $d = 97131$ and calculate the matrix

$$Q = A^{97131} \bmod 199867 = \begin{bmatrix} 146146 & 303 & 187134 \\ 97027 & 71586 & 196024 \\ 58367 & 115209 & 91566 \end{bmatrix}.$$

- Publish the public key $[A, 36987216, 97131, Q]$.

B. Alice's encryption steps

- Acquire Bob's public key $[A, 36987216, 97131, Q]$.
- After selecting an integer $u = 3925$, Alice calculates the matrixes C and D with Bob's public key,

$$C = A^{3925} \bmod 199867 = \begin{bmatrix} 185342 & 188610 & 107335 \\ 147092 & 59828 & 86685 \\ 61984 & 128955 & 156400 \end{bmatrix},$$

$$D = Q^{3925} \bmod 199867 = \begin{bmatrix} 158335 & 135371 & 118290 \\ 180294 & 148209 & 128784 \\ 175149 & 105464 & 125418 \end{bmatrix}.$$

- Let the matrix M be the plaintext. She can calculate the cipher text matrix E.

$$M = \begin{bmatrix} 136164 & 75845 & 166248 \\ 100495 & 141799 & 85721 \\ 60882 & 37905 & 38660 \end{bmatrix},$$

$$E = (D \times M) \bmod 199867 = \begin{bmatrix} 158976 & 121301 & 187224 \\ 108166 & 176611 & 42960 \\ 95740 & 189640 & 129183 \end{bmatrix}.$$

- Send the encrypted data $[C, E]$ to Bob.

C. Bob's decryption steps

Bob performs the following steps after receiving Alice's encrypted data $[C, E]$.

- Calculate the matrix D with his private key $d = 97131$.

$$D = C^{97131} \bmod 199867 = \begin{bmatrix} 158335 & 135371 & 118290 \\ 180294 & 148209 & 128784 \\ 175149 & 105464 & 125418 \end{bmatrix}.$$

- Compute the matrix

$$D_{199867}^{-1} = \begin{bmatrix} 5668 & 103764 & 100957 \\ 19960 & 146800 & 40609 \\ 75844 & 105348 & 165025 \end{bmatrix}.$$

- Bob recovers the plaintext, $M = (D_{199867}^{-1} \times E)$

$$\bmod 199867 = \begin{bmatrix} 136164 & 75845 & 166248 \\ 100495 & 141799 & 85721 \\ 60882 & 37905 & 38660 \end{bmatrix}.$$

VI. ANOTHER EXAMPLE

To verify the correctness and rationality of the proposed cryptosystem, another example is carried out using the digital image Lena. The detailed description is given as follows.

A. Experimental steps

(1) Bob's key-generating steps

- Choose the digital image Tiffany as the matrix $A_{512\times512}$ and the prime $p = 256$, as shown in Fig.1.

Figure 1. Tiffany

- Because there are 512×512 elements in $A_{512\times512}$ and the element $a_{i,j} \in \{0, 1, 2, \cdots, 255\}$, the period T of $A \bmod 256$ is a big-integer and $T \le 2^{8\times512\times512}$.
- Randomly choose the private key $d = 44536346\ 54354354543543543454 \approx 2^{92}$ and calculate the matrix $Q = A^d \bmod 256$. The result of Q is as shown in Fig. 2.

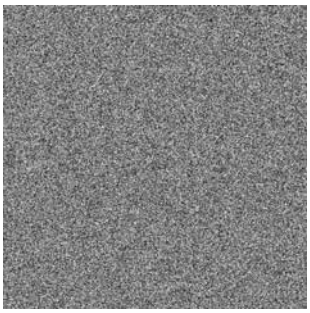

Figure 2. Q matrix

- Publish the public key $[A,T,p,Q]$.

(2) Alice's encryption steps

- Acquire Bob's public key $[A,T,p,Q]$.
- After randomly selecting an integer $u = 57435435\ 43543543345799853845$, Alice calculates the matrixes $C = A^u \mod 256$ and $D = Q^u \bmod 256$ with Bob's public key. The results of C, D are respectively as shown in Fig. 3 and Fig. 4.

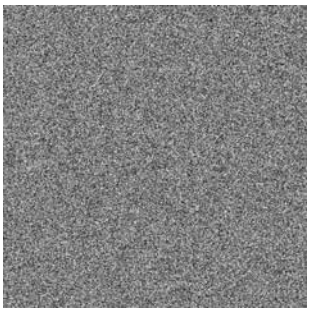

Figure 3. C matrix

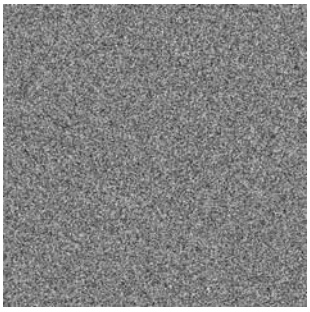

Figure 4. D matrix

- Let the digital image Lena be the plaintext $M_{512\times512}$, as shown in Fig. 5. She can calculate the cipher text matrix $E = (D \times M) \bmod 256$. E is the encrypted image, as shown in Fig. 6.
- Send the encrypted data $[C,E]$ to Bob.

(3) Bob's decryption steps

Bob performs the following steps after receiving Alice's encrypted data $[C,E]$.

Figure 5. Lena

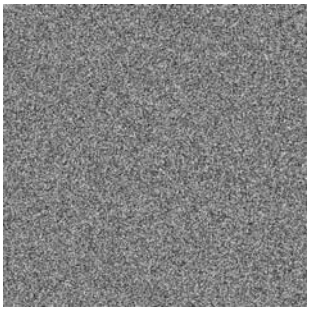

Figure 6. Encrypted image

- Calculate the matrix $D = C^d \bmod 256$ with his private key $d = 44536346543543545435435434 5 \approx 2^{92}$.
- Compute the matrix D_p^{-1}, and the result is as shown in Fig. 7.

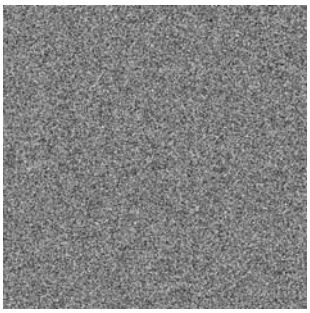

Figure 7. The inverse matrix of D

- Bob recovers the original image by computing $M = (D_p^{-1} \times E) \bmod 256$, and the result is as shown in Fig. 8.

Figure 8. Decrypted image

B. Robustness analysis

The correlation coefficient between two images with the same size is defined as follows [22],

$$\rho_{XY} = \frac{\mathrm{cov}(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}}, \quad (3)$$

where X and Y are gray images, $E(X) = \frac{1}{N}\sum_{i=1}^{N} x_i$, $\mathrm{cov}(X,Y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(X)][y_i - E(Y)]$, $D(X) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(X)]^2$, N is the pixel number of the images X and Y, $x_i \in X$ and $y_i \in Y$ are two pixels in the corresponding position.

NPCR (Number of Pixels Change Rate) between two images with the same size is defined as follows [23],

$$f(i,j) = \begin{cases} 0 & X(i,j) = Y(i,j) \\ 1 & X(i,j) \neq Y(i,j) \end{cases}, \quad (4)$$

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} f(i,j)}{m \times n} \times 100\%, \quad (5)$$

where $X_{m\times n}$ and $Y_{m\times n}$ are images.

UACI (Unified Average Changing Intensity) between two images with the same size is defined as follows [23],

$$UACI = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} |X(i,j) - Y(i,j)|}{255 \times m \times n} \times 100\%, \quad (6)$$

where $X_{m\times n}$ and $Y_{m\times n}$ are images.

With the criterions of correlation coefficient, NPCR and UACI, we analyze the robustness of the proposed cryptosystem as follows.

(1) Without noise effect

Supposing that the encrypted image isn't damaged during the storage or transmission, the decrypted image is the same as the original image. Therefore, for the decrypted image and original image, the correlation coefficient is ρ_{XY} =1, $NPCR$ =0 and $UACI$ =0.

(2) Salt and peppers noise attack

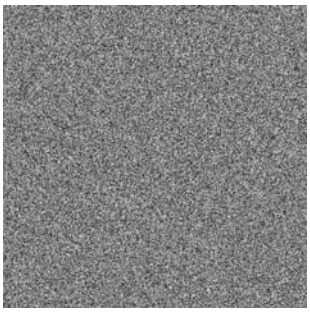

Figure 9. Salt and peppers noise (0.03)

To simulate the noise channel, we add the salt and peppers noise (0.03) to the encrypted image, as shown in Fig. 9. The corresponding decrypted image is as shown in Fig. 10. Finally, for the decrypted image and original image, the correlation coefficient is ρ_{XY} = 0.8855, $NPCR$ =9.841% and $UACI$ = 7.91%. Therefore, the new cryptosystem are robust against the salt and peppers noise attack.

Figure 10. Decrypted image

(3) Cutting attack

To simulate the tampering operation during the storage or transmission, we cut the encrypted image (6.25%), and the tampered image is as shown in Fig. 11. The corresponding decrypted image is as shown in Fig. 12. Finally, for the decrypted image and original image, the correlation coefficient is ρ_{XY} = 0.8877, $NPCR$ =12.45% and $UACI$ = 2.84%. Therefore, the new cryptosystem are robust against the cutting attack.

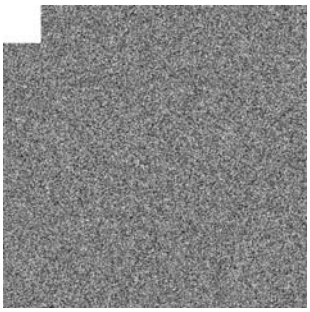

Figure 11. Cutting (6.25%)

Figure 12. Decrypted image

C. Encryption efficiency analysis

(1) Encryption efficiency analysis of ECC

The bottom-layer operations of ECC are the big-integer operations, such as big-integer addition, big-integer subtraction, big-integer multiplication and big-integer division. The core operation of ECC is the scalar multiplication operation. People have proposed some fast algorithms, such as the binary method, non-adjacent form (NAF) method and sliding window method. We realize the ElGamal scheme of ECC [15] with the binary method.

The algorithms were programmed in MyEclipse 7.5 on a PC with the Intel (R) Pen 4, CPU frequency 2.80 Ghz and Memory 2 GB.

Choose the 192 bits elliptic curve, which is recommended by NIST. The parameters of this elliptic curve are $a=-3$, $b=$ 245515554600894381774029391519745178476910805816119123806 5, and $p=$ 6277101735386680763835789423176059013767194773182842284081. The base point is $N=$ (602046282375688656758213480587526111916698976636884684818, 174050332293622031404857552280219410364023488927386650641), the period of N is $T=$ 6277101735386680763835789423176059013767194773182842284081. The private key is $d=$ 1000072627282998656287642690503854234 53895943703. To encrypt a pixel value with ECC, the encrypted time is about 42.1637 ms $\approx$ 42 ms. Therefore, to encrypt Lena $A_{512\times512}$ with ECC, the total encrypted time is about $42\times512\times512\approx11010$ s ≈3.0583 h.

(2) Encryption efficiency analysis of the proposed cryptosystem

The core operations of the proposed cryptosystem are multiplication of matrices and module operations, and we offer a fast algorithm in Section IV(A). The algorithms were programmed in Matlab 6.5 on a PC with the Intel (R) Pen 4, CPU frequency 2.80 Ghz and Memory 2 GB. The encrypted time in experiment is 43.0531 s. Therefore, the proposed cryptosystem is efficient to satisfy the requirement in the practical application.

VII. Efficiency Analysis

By comparing the difference between one-dimension DLP and two-dimension DLP, we analyze the temporal complexity of the new cryptosystem in detail as follows.

A. One-dimension DLP

Let $\langle\alpha\rangle$ denotes the group generated by a number $\alpha \bmod p$, where p is a prime or $p=2^m$. Suppose the order of $\langle\alpha\rangle$ is T_1. If Oscar (the attacker) adopts the brute-force attack, the worst case is that he should compute $\alpha^2=(\alpha\times\alpha) \bmod p$, $\alpha^3=(\alpha^2\times\alpha) \bmod p$, $\cdots$, $\alpha^{T_1}=(\alpha^{T_1-1}\times\alpha) \bmod p$. Under the premise of known the value of α^k, he only needs one time of multiplication operation ($\alpha^k\times\alpha$) and one time of modular operation ($\alpha^{k+1} \bmod p$) to obtain the value of $a^{k+1}=(\alpha^k\times\alpha) \bmod p$.

B. Two-dimension DLP

Let $\langle A\rangle$ denotes the group generated by a matrix $A_{n\times n} \bmod p$, where p is a prime or $p=2^m$. Supposed the order of $\langle A\rangle$ is T_2. If Oscar adopts the brute-force attack, the worst case is that he should compute $A^2=(A\times A) \bmod p$, $A^3=(A^2\times A) \bmod p$, $\cdots$, $A^{T_2}=(A^{T_2-1}\times A) \bmod p$. Under the premise of known the value of A^k, he needs to compute the elements of A^{k+1} at first to obtain the result of $A^{k+1}=(A^k\times A) \bmod p$. According to the matrix theory, we have $a_{ij}^{k+1}=a_{i1}^k\times a_{1j}+a_{i2}^k\times a_{2j}+\cdots+a_{in}^k\times a_{nj}$, where $a_{ij}^{k+1}\in A^{k+1}$, $a_{ij}^k\in A^k$ and $a_{ij}\in A$. Therefore, to obtain the value of the element a_{ij}^{k+1}, we need n times of multiplication operation, $n-1$ times of addition operation and one time of modular operation ($a_{ij}^{k+1} \bmod p$). In total, under the premise of known the value of A^k, to obtain the result of $A^{k+1}=(A^k\times A) \bmod p$, he needs $n^2\times n=n^3$ times of multiplication operation, $n^2(n-1)$ times of addition operation and n^2 times of module operation.

From the above analysis, we can see that solving the two-dimension DLP is more different than the one-dimension DLP. The temporal complexity of two-dimension DLP is n^2 times at least of one-dimension DLP. Therefore, for the same security level, the key length of the proposed cryptosystem is $1/n^2$ of the cryptosystems based on the one-dimension DLP in theory. In this sense, the key length of the new cryptosystem is shorter than the public-key cryptosystem based on the one-dimension DLP, such as Diffie-Hellman key exchange [7], Elgamal [24] and Massey-Omura [25].

To verify the above conclusion, several experiments are also performed. Let the generator of the group $\langle A\rangle$ be

$$A=\begin{bmatrix}4&7&1\\6&4&8\\9&6&4\end{bmatrix}.$$

We calculated the orders T of $\langle A\rangle$ for $p=163$, $p=1987$ and $p=199867$ respectively, as shown in Tab.1. Supposing that Oscar adopts the brute-force attack, the time needed for the worst case to attack one-dimension DLP and two-dimension DLP is shown in Tab. 1.

TABLE 1.
COMPARISON ON THE SPEED FOR ATTACKING ONE-DIMENSION DLP AND TWO-DIMENSION DLP.

p	T	Time for one-dimension DLP (s)	Time for two-dimension DLP (s)
163	$26568\approx2^{15}$	0.0047	0.0734
1987	$3948168\approx2^{22}$	0.5938	11.3594
199867	$36987216\approx2^{25}$	5.5620	107.1880

VIII. Security Analysis

A. Possible attack analysis

The security of the new public-key cryptosystem is based on the hardness of solving the two-dimension DLP. To illuminate the cryptosystem security, we consider the following three possible attacks.

(1) Attack 1

- Attack: Oscar tries to obtain Bob's private key d from Bob's public key $[A,T,p,Q]$.

- Attack analysis: From the principle of the public-key cryptosystem, Bob publishes his public key $[A,T,p,Q]$. Therefore, Oscar is available to obtain $[A,T,p,Q]$. From the steps of the new cryptosystem, we have $Q = A^d \bmod p$. Oscar is required to calculate $d = \log_A Q$. Therefore, obtaining Bob's private key d is equivalent to solving the two-dimension DLP.

(2) Attack 2

- Attack: Supposing that Oscar has obtained Bob's public key $[A,T,p,Q]$ and the cipher text $[C,E]$, he tries to compute Bob's private key d.
- Attack analysis: From the principle of the public-key cryptosystem, Oscar is available to obtain $[A,T,p,Q]$. We suppose that Oscar can obtain the cipher text $[C,E]$ fortunately. From the steps of the new cryptosystem, we have $C = A^u \bmod p$, i.e., $u = \log_A C$. He can calculate $D = Q^u \bmod p = C^d \bmod p$ with Bob's public key Q. Finally, he can compute $d = \log_C D$. During the whole process, Oscar should compute $u = \log_A C$ and $d = \log_C D$. Therefore, to obtain Bob's private key d, unless Oscar can solve the two-dimension DLP.

(3) Attack 3

- Attack: Supposing that Oscar has obtained Bob's public key $[A,T,p,Q]$ and the cipher text $[C,E]$, he tries to gain Alice's plaintext M.
- Attack analysis: From the principle of the public-key cryptosystem, Oscar is available to obtain $[A,T,p,Q]$. We suppose that Oscar can obtain the cipher text $[C,E]$ fortunately. From the steps of the new cryptosystem, we have $C = A^u \bmod p$, i.e., $u = \log_A C$. He can calculate $D = Q^u \bmod p$ with Bob's public key Q. Then he can compute D^{-1}. Finally, he can compute $M = (D^{-1} \times E) \bmod p$ with the plaintext E. Oscar needs to compute $u = \log_A C$ during the attack process. Therefore, to obtain Alice's plaintext M, unless the two-dimension DLP is solved.

The above analysis demonstrates that the difficulty of breaking our cryptosystem is equivalent to breaking the Elgamal cryptosystem and solving the two-dimension DLP.

B. Key space analysis

The key space is a set comprised of all the possible keys. For a secure image encryption algorithm, the key space should be large enough to make the brute force attack infeasible [26].

(1) Key space analysis of the cryptosystem based on the one-dimension DLP

Because the integer a are chosen from the set $Z_p = \{0,1,2,\cdots,p-1\}$ in the cryptosystems based on the one-dimension DLP, there are p possible cases of a. Therefore, the period T of the generator $a \bmod p$ is an integer which is not more than p. Since the private key d is randomly chosen from the set $\{1,2,\cdots,T-1\}$, the size of the key space is not over p.

(2) Key space analysis of the proposed cryptosystem

Because the elements of the matrix $A_{n\times n}$ are from the set $Z_p = \{0,1,2,\cdots,p-1\}$ in the new cryptosystem, there are $p^{n\times n}$ possible cases of $A_{n\times n}$. Therefore, the period T of the generator $A_{n\times n} \bmod p$ is an integer which is not over $p^{n\times n}$. Since the private key d is randomly chosen from the set $\{1,2,\cdots,T-1\}$, the size of the key space is not more than $p^{n\times n}$. For example, in the second example, the size of the key space is a big integer and not more than $2^{8\times 512\times 512}$.

In this sense, the key space $p^{n\times n}$ of the new cryptosystem is larger than the key space p of the public-key cryptosystem based on the one-dimension DLP. Therefore, the proposed cryptosystem possesses the advantage of high security.

IX. CONCLUSIONS

The definition of DLP is generalized from one dimension to two dimensions, and then a new public-key cryptosystem based on the two-dimension DLP is proposed, which generalizes the public-key cryptosystem from one dimension to two dimensions. The core algorithms of the new cryptosystem are offered, including fast algorithm, the algorithm of computing the inverse matrix modulo p, and the algorithm of finding the period T. Especially, to improve the efficiency, the square-multiply method for numbers is generalizing to matrixes. The theory analysis and experimental data show that the proposed cryptosystem possesses the advantages of the outstanding robustness, short key length, high security and encrypting many data once.

ACKNOWLEDGEMENTS

The authors like to express their sincere thanks to the anonymous reviewers and the editor P. Mahanti of Journal of Computers for their constructive comments and suggestions.

The authors thank Professor Xinqing Yan who works in North China University of Water Conservancy and Electric Power, for his careful reviews and valued suggestions. The authors also thank Ph.D. Jie Gai from Cameroon for pointing out several grammar mistakes.

REFERENCES

[1] Andrzej Chmielowiec, "Fixed points of the RSA encryption algorithm," *Theoretical Computer Science*, vol. 411, pp. 288–292, January 2010.

[2] Wongoo Lee, and Jaekwang Lee, "Design and implementation of secure e-mail system using elliptic curve cryptosystem," *Future Generation Computer Systems*, vol. 20, pp. 315–326, February 2004.
[3] Tzer-Shyong Chen, Kuo-Hsuan Huang, and Yu-Fang Chung, "A practical authenticated encryption scheme based on the elliptic curve cryptosystem," *Computer Standards & Interfaces*, vol. 26, pp. 461–469, May 2004.
[4] Coron JS, Naccache D, and Desmedt Y, "Index calculation attacks on RSA signature and encryption," *Designs, Codes and Cryptography*, vol. 38, pp. 41–53, January 2006.
[5] Tzer-Shyong Chen, "A specifiable verifier group-oriented threshold signature scheme based on the elliptic curve cryptosystem," *Computer Standards & Interfaces*, vol. 27, pp. 33–38, January 2004.
[6] Chen TS, Chung YF, and Huang GS, "Efficient proxy multisignature schemes based on the elliptic curve cryptosystem," *Computers & Security*, vol. 22, pp. 527–534, June 2003.
[7] Diffie, W., Hellman, M, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, June 1976.
[8] Rivest, R., Shamir, and A., Aldeman, L, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, February 1978.
[9] Hung-Min Sun, Mu-En Wu, M. Jason Hinek, Cheng-Ta Yang, and Vincent S. Tseng, "Trading decryption for speeding encryption in rebalanced-RSA," *The Journal of Systems and Software*, vol. 82, pp. 1503–1512, September 2009.
[10] V. Miller, "Uses of elliptic curves in cryptography," *Advances in Cryptology-Crypto'85*, Berlin: Springer-Verlag, pp. 417–426, 1985.
[11] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–209, July 1987.
[12] Fu Minfeng, and Chen Wei, "Elliptic curve cryptosystem ElGamal encryption and transmission scheme," *International Conference on Computer Application and System Modeling*, vol. 6, pp. 51–53, June 2010.
[13] Tzer-Shyong Chen, "A threshold signature scheme based on the elliptic curve cryptosystem," *Applied Mathematics and Computation*, vol. 162, pp. 1119–1134, March 2005.
[14] J.A. Muir, D.R. Stinson, "On the low hamming weight discrete logarithm problem for nonadjacent representations," *Applicable Algebra in Engineering, Communication and Computing*, vol. 16, pp. 461–472, June 2006.
[15] Guiliang Zhu, and Xiaoqiang Zhang, "Mixed image element encryption algorithm based on an elliptic curve cryptosystem," *Journal of Electronic Imaging*, vol. 17, pp. 023007.1–5, February 2008.
[16] Dong Fuguo, and Li Yurong, "Study on QinJiuShao algorithm and its application in RSA," *Computer Engineering and Applications*, vol. 44, pp. 65–78, June 2008. (in Chinese)
[17] Adleman L M, "Factoring numbers using singular integers," *The 23rd Annual ACM Symposium on the Theory of Computing*, New Orleans, pp. 64–71, 1991.
[18] Li Qiang, and Zhang Jiyong, "A new fast RSA algorithm," *Mini-Micro Systems*, vol. 22, pp. 70–72, January 2001.
[19] Bergeron F, J. Berstel, S. Brlek, and C. Duboc, "Addition chains using continued fractions," *Journal of Algorithms*, vol. 10, pp. 403–412, October 1989.
[20] Hao Yuanling, and Ma Shiwei, "Fast optimization algorithm for scalar multiplication in the elliptic curve cryptography over prime field," *Lecture Notes in Computer Science*, vol. 5226, pp. 904–911, February 2008.
[21] Tao Ran, and Chen Liyan, "Fast algorithm for scalar multiplication in elliptic curve cryptography," *Transactions of Beijing Institute of Technology*, vol. 25, pp. 701–704, August 2005.
[22] Hongjun Liu, and Xingyuan Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Journal of Computational and Applied Mathematics*, vol. 59, pp. 3320–3227, October 2010.
[23] C. K. Huang, and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Optics Communications*, vol. 282, pp. 2123–2127, November 2009.
[24] T. EIGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, March 1985.
[25] N. P. Smart, "The discrete logarithm problem on elliptic curves of trace one," *Journal of Cryptology*, vol. 12, pp. 193–196, December 1999.
[26] N. K. Pareek, Vinod Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing*, vol. 24, pp. 926–934, September 2006.

Xiaoqiang Zhang. He was born in 1983 in Neihuang county, Henan province, China. He is a doctor candidate at state key lab of software development environment, Beihang University. His research interests include information security, encryption theory, image encryption, digital watermarking, and software engineering.

Guiliang Zhu. He graduated at Peking University in 1977. He was born in 1950 in Zhongmou county, Henan province, China. Professor Zhu is a master supervisor at North China University of Water Conservancy and Electric Power (NCWU). His current research interests include information security, encryption algorithm, software engineering, operating system.

Weiping Wang. She is a master candidate at Department of Information Engineering, NCWU. She was born in 1985. Her research interests include software engineering, image encryption.

Mengmeng Wang. She is a master candidate at Department of Information Engineering, NCWU. She was born in 1988. Her research interests include software engineering, image encryption, encryption theory.

Shilong Ma. Professor Ma is a doctor supervisor at school of computer science and engineering, Beihang University. He was born in 1953. His research interests include calculating model on the network environment, dynamic statistic behavior of logic and computation, calculating model of massive data process, grid computing technology and application.