# 改良式機率加密法
# An Improvement on a Probabilistic Encryption Scheme

張真誠和祖善明
Chang, C.C. and Tsu, S.M.

國立中正大學資訊工程系
Department of Computer Science and Information Engineering,
National Chung Cheng University, Chiayi,Taiwan 621, R.O.C
E-mail: ccc@cs.ccu.edu.tw

## 摘要

*在本文中我們改良Harn和Kiesler的機率式加密法。我們的方法是利用公開金匙和每次遞回地加密二個位元的概念，使得明文擴張的程度與Harn和Kiesler的方法一樣，但我們的加解密法卻比他們的方法快兩倍。*

關鍵字：機率式加密法，公開金匙密碼系統。

## Abstract

*In this letter, we make an improvement on Harn and Kiesler's probabilistic encryption scheme. An efficient probabilistic encryption scheme is then proposed. Our scheme utilizes the concept of public keys and recursively encrypts two bits at a time. The message bit expansion in our scheme is the same as Harn and Kiesler's scheme. On the other hand, the time for enciphering and deciphering is twice as fast as Harn and Kiesler's.*

Keywords: probabilistic encryption scheme, public-key cryptosystem.

## 1.Introduction

The public key cryptosystem was introduced by Diffie and Hellman [1] in their original paper in 1976. Later, many known schemes were quickly proposed to implement it, such as RSA scheme [6] in 1978. In 1987, Goldwasser and Micali [2] pointed out some basic problems with some schemes so far presented; for example, the same message is always only one encrypted form whenever it is sent to someone in RSA scheme; they proposed a new approach called probabilistic encryption as an alternative approach which can strengthen the security. Probabilistic encryption schemes result in many possible encrypted forms that are corresponding to the same message.

The first probabilistic encryption scheme proposed by Goldwasser and Micali was inefficient. It required the encryption of every bit of message independently, that scheme caused a message bit expansion of 1:K, where K is called the security parameter. Jingmin and Kaicheng [4] proposed a new way to encrypt a sequence of the individual message bits of length L, with a low message bit expansion of (L+K-1)/L, where K is the security parameter. More recently, Harn and Kiesler [3] also presented an elegant way based on quadratic residue theory to achieve the probabilistic encryption. In their scheme, Harn and Kiesler obtained the ciphertext by recursively encrypting one message bit at a time, with the same message bit expansion of Jingmin and Kaicheng's scheme.

In this letter, we make an improvement of Harn and Kiesler's probabilistic encryption scheme. By our method, the encryption and decryption operations are twice as fast as theirs while providing slightly better message bit expansion of (L+K-2)/L, where K is the security parameter and L is the length of plain message.

## 2.Quadratic Residue Theory

In what follows, we use the symbol $QR_n$ to represent the set of all integers between 1 and n-1 that are quadratic residues modulo n, and the symbol $QNR_n$ to represent those that are quadratic nonresidues modulo n. We use the symbol L(a/p) for the Legendre symbol, where p is an odd prime and $1 \leqq a \leqq n-1$. The symbol J(a/n) is used to represent as the Jacobi symbol, where n is a product of two large primes. For p and q two primes, an integer $a \in QR_p \cap QR_q$ means that a is quadratic residue modulo p and is quadratic residue modulo q. Similarly, the cases are for $a \in QR_p \cap QNR_q$, $a \in QNR_p \cap QR_q$ and $a \in QNR_p \cap QNR_q$, respectively.

Theorem 2.1 [Harn and Kiesler 1990]

For any integer N=PQ, with P and Q primes of the form 4k+3. An integer $a \in QR_N$, the four square roots of a are distinguishable among four different cases as specified in any of the following ways:

Case(1): $root \in QR_P \cap QR_Q$,

Case(2): $root \in QR_P \cap QNR_Q$,

Case(3): $root \in QNR_P \cap QR_Q$,

Case(4): $root \in QNR_P \cap QNR_Q$.

or

Case(1): $J(root/N) = 1$ and root is odd,

Case(2): $J(root/N) = 1$ and root is even,

Case(3): $J(root/N) = -1$ and root is odd,

Case(4): $J(root/N) = -1$ and root is even.

Any user who knows the factorization of N can use the above theorem to distinguish any solution of the square roots of $x^2 = a$ mod N, where $a \in QR_N$. Alternatively, when the factorization of N is known, then the desired root, among four roots of the congruence $x^2 = a$ mod N, can be specified according to J(root/N) and the characteristic odd or even of the root.

## 3.Our Probabilistic Encryption Scheme

**Secret key:** Every user $U_i$ needs to select a pair of two large distinct primes ($P_i, Q_i$), as his secret key, where $P_i$ and $Q_i$ are of the form 4k+3. Then he calculates $n_i = P_i Q_i$.

**Public key:** Every user $U_i$ selects four parameters $\alpha$, $\beta$, $\gamma$, and $\lambda$, such that $\alpha \in QR_{P_i} \cap QR_{Q_i}$, $\beta \in QR_{P_i} \cap QNR_{Q_i}$, $\gamma \in QNR_{P_i} \cap QR_{Q_i}$, and $\lambda \in QNR_{P_i} \cap QNR_{Q_i}$. Then the user $U_i$ publishes $(n_i, \alpha, \beta, \gamma, \lambda)$ as his public key.

**Encryption:** Any user $U_j$ who wants to send a binary message string m $= m_1 \ m_2 \ldots m_L$ to user $U_i$ needs to randomly select an integer x within the range $[1, n_i - 1]$, such that GCD(x, $n_i$)=1, where $n_i$ is user $U_i$'s public key and L is the length of binary message. A probabilistic encryption algorithm is given below.

Initial Step: Set C=x, j=1

Step1:Compute

$$C = C^2 \times TYPE(m_{2j-1}, m_{2j}) \bmod n_i,$$

where the function TYPE(a,b) is defined as below:

$$TYPE(a,b) = \begin{cases} \alpha & if\ a = 0,\ b = 0, \\ \beta & if\ a = 0, b = 1, \\ \gamma & if\ a = 1, b = 0, \\ \lambda & if\ a = 1, b = 1. \end{cases}$$

Step2:Compute $b_{2j-1} = m_{2j-1} \oplus m_{2j}$, where $\oplus$ is the exclusive-or operater.

Step3:Compute $b_{2j}$ according to the following rule:

$$b_{2j} = \begin{cases} 0 & if\ C\ is\ even, \\ 1 & if\ C\ is\ odd. \end{cases}$$

Step4:Repeat from Step 1 to Step3 until j =j+1>L.

Therefore, the user $U_j$ obtains the ciphertext C and (L-2) binary bits $b_1 \ b_2 \ldots b_{L-2}$. Then he transmits them to the user $U_i$. For the receiver $U_i$, the corresponding decryption algorithm is given below.

**Decryption:** Once user $U_i$ receives the ciphertext C and a binary sequence B=$b_t \ b_{t-1} \ldots b_1$ with length t, he will start to decipher the message recursively.

Initial Step: Compute L=BinaryLength(B)+2, where the function BinaryLength(string) can obtain the length of the given binary string.

Step 1:Compute the message bit $m_{L-1}$ as follows. $m_{L-1} = \begin{cases} 0 & if\ C \in QR_{Pi}, \\ 1 & if\ C \in QNR_{Pi}. \end{cases}$

Step 2:Compute the message bit $m_L$ as follows.

$$m_L = \begin{cases} 0 & if\ C \in QR_{Q_i}, \\ 1 & if\ C \in QNR_{Q_i}. \end{cases}$$

Step 3:Find the specified root of the congruence

$x^2 = C \times (TYPE(m_{L-1}, m_L))^{-1} \bmod n_i$ according to the following rules:

$$\text{specified root} = \begin{cases} J(\text{root}/n_i) = 1 \text{ and root is odd} \\ \quad \text{if } b_{L-3} = 0, b_{L-2} = 1, \\ J(\text{root}/n_i) = 1 \text{ and root is even} \\ \quad \text{if } b_{L-3} = 0, b_{L-2} = 0, \\ J(\text{root}/n_i) = -1 \text{ and root is odd} \\ \quad \text{if } b_{L-3} = 1, b_{L-2} = 1, \\ J(\text{root}/n_i) = -1 \text{ and root is even} \\ \quad \text{if } b_{L-3} = 1, b_{L-2} = 0. \end{cases}$$

Step 4:Set C = the root found in Step3. Repeat from Step1 to Step 3 until L=L-2<2.

**Example 3.1**

Assume that user $U_i$'s secret key $(P_i, Q_i)$=(11,19) and the associated public key ($n_i$, $\alpha, \beta, \gamma, \lambda$)=(209,1,59,43,41). Given a message M=171 = $(10101011)_2$, the encryption procedure is processed as follows.

1. Since $m_1$=1 and $m_2$ =0 , then the ciphertext C is computed as below:

   $$C = 139^2 \times TYPE(1,0) \bmod 209$$
   $$= 139^2 \times 43 \bmod 209$$
   $$= 28.$$

   $b_1 = m_1 \oplus m_2$ =1⊕0=1, and $b_2$=0 since 28 is even.

2. Since $m_3$=1 and $m_4$=0, similarly, C is computed as below:

   $$C = 28^2 \times 43 \bmod 209 = 63 .$$

   $b_3 = m_3 \oplus m_4 = 1$ and $b_4$=1 since 63 is odd.

3. Since $m_5$=1 and $m_6$=0, then C is computed as below:

   $$C = 63^2 \times 43 \bmod 209 = 123 .$$

   $b_5 = m_5 \oplus m_6 = 1$ and $b_6$=1 since 123 is odd.

4. Since $m_7$=1 and $m_8$=1, then C is computed as below:

   $$C = 123^2 \times 41 \bmod 209 = 186 .$$

The ciphertext C = 186 and a binary sequence $b_6\, b_5 \dots b_1$=111101 are then transmitted.

**Example 3.2**

Given the ciphertext C=186 and a binary sequence $b_6\, b_5 \dots b_1$=111101, the decryption is processed as below:

1. Since $186 \in QNR_{11} \cap QNR_{19}$, $m_7$=1 and $m_8$=1 are obtained. Owing to $b_5$=1 and $b_6$=1, the specified solution of $x^2 = 186 \times TYPE(1,1)^{-1} \bmod 209$ is 123.
2. Since $123 \in QNR_{11} \cap QR_{19}$, $m_5$=1 and $m_6$=0 are obtained. Owing to $b_3$=1 and $b_4$=1, the specified solution of $x^2 = 123 \times TYPE(1,0)^{-1} \bmod 209$ is 63.
3. Since $63 \in QNR_{11} \cap QR_{19}$, $m_3$=1 and $m_4$=0 are obtained. Owing to $b_1$=1 and $b_2$=0, the specified solution of $x^2 = 63 \times TYPE(1,0)^{-1} \bmod 209$ is 28.
4. Since $28 \in QNR_{11} \cap QR_{19}$, $m_1$=1 and $m_2$=0 are obtained.

Therefor, M= $m_1\, m_2 \dots m_8$= $(10101011)_2$ is then obtained.

## 4. Security Analysis

The security of our scheme is the same as that of Harn and Kiesler's. It is based on the difficulty of finding square roots of a quadratic residue modulo an integer which is a product of two large prime numbers. Rabin [5] proved that such a problem is equivalent to factorization of an integer which is a product of two large prime numbers. As we know, so far the problem of factorization is still computationally infeasible.

It needs to be pointed out that any user can check the Jacobi symbol of C without knowing the factorization of the public key $n_i$. However, no information would be revealed about the message bits by checking the Jacobi symbol of C since $J(\alpha / n_i) = J(\lambda / n_i) = 1$ and $J(\beta / n_i) = J(\gamma / n_i) = -1$ ; therefore, the probability of guessing the plaintext correctly is about $(\frac{1}{2})^{L/2}$, where L is the binary string length of the plain message.

## 5.Conclusions

In this letter, an improvement of the probabilistic encryption scheme proposed by Harn snd Kiesler is made and a more efficient method for encryption and decryption is also presented. The difference between our scheme and that of Harn and Kiesler's is that we encrypt two message bits at a time. In each encryption, only one multiplication operation is used, thus only half of the multiplication operations of that Harn and Kiesler used are needed in our scheme. On the other hand, two message bits are recovered at a time by solving a quadratic congruence, it is also twice as fast as Harn and Kiesler's. Thus, for the same message string, the time for encryption and decryption needed by our scheme is twice as fast as Harn and Kiesler's. Further, our scheme also provides slightly better message bit expansion of (L+K-2)/L then that of Harn and Kiesler's, where K is the security parameter and L is the length of plain message.

## References

[1] Diffie, W., and Hellman, M. E.:"New directions in cryptofraphy", *IEEE Inform. Theory*, 1976, IT-22, pp. 644-654.

[2] Goldwasser, S. and Micali, S.:"Probabilistic encryption", *J. Comput. Syst. Sci.*, 1984, 28, pp.270-299.

[3] Harn, L. and Kiesler, T.:"An efficient probabilistic encryption scheme", *Information Processing Letters*, vol. 34, 1990, pp. 123-129.

[4] Jingmin and Kaicheng, L.:"A new probabilistic encryption scheme", *Eurocrypt'88*, 1988, pp.415-418.

[5] Rabin, M. O.:"Digitalized signatures and public key functions as intractable as factorization", *MIT/LCS/TR-212*, January 1979.

[6] Rivest, R. L., Shamir, A., and Adelman, L.:"A method for obtaining digital signatures and public-key cryptosystem", *Commun. ACM*, 1978, 21, (2), pp. 120-126.