A NEW PROBABILISTIC ENCRYPTION SCHEME

He Jingmin and Lu Kaicheng
Dept. of Computer Science, Tsinghua University
Beijing, People's Republic of China

Abstract. In this paper we present a new probabilistic public key cryptosystem. The system is polynomially secure. Furthermore, it is highly efficient in that it's message expansion is 1+(k-1)/1, where k is the security parameter and 1 the length of the encrypted message. Finally, the system can be used to sign signatures.

1. Introduction

The most important problem in modern cryptography is how to encrypt messages in a secure and efficient way. Here two things are of equal importance: security and efficiency.Up to now three different notions of security have been proposed: Goldwasser and Micali's polynomial security, semantic security [1], and Y-security introduced by Yao [2]. Micali et al([3]) have pointed out that these three notions are essentially equivalent. In this paper we'll adopt the notion of polynomial security. As to the efficiency, it usually means the encrypting and decrypting time and the message expansion.

The earliest public key cryptosystem is RSA [4]. RSA is highly efficient because it's message expansion is about one (the possiblely least value). However, it's security remains to be proven. Actually RSA is a deterministic cryptosystem and can't be secure according to [1]. In another direction, Goldwasser and Micali [1] presented the first probabilistic encryption scheme whose polynomial security is rigorously proven. But their scheme is not efficient at all. They encrypt every bit of the message independently, so the message expansion is k (the security parameter) and this makes the scheme totally unvalued in practice.

In this paper we concern both security and efficiency. We present a new "random iterative encryption scheme" which can achieve both polynomial security and high efficiency. The idea is simple: we randomly and iteratively encrypt the plaintext bit by bit. In this way we can get a secure public key cryptosystem with a low message expansion of 1+(k-1)/1, where 1 is the length of the plaintext and k the security par-

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 415-418, 1988.

ameter. The one more lucky thing is that the new scheme can be used to sign digital signatures, which seems impossible in the schemes of [1], [5] and [6].

Remark: Blum and Goldwasser have presented another secure probabilistic encryption method with a message expansion of 1+k/l. Their method is similar to that of Blum et al.([5]), in which it exlusive-or the plaintext with a sequence of the same length generated by a pseudo-random number generator. For the details see [5] and [6].

2. Background

Let N denote the set of positive integers and $n \in N$. Let $Z_n^+ = \{x \mid 1 \leq x < n \text{ and } (x,n) = 1\}$, $Z_n^1 = \{x \mid 1 \leq x < n \text{ and } (x/n)=1\}$, where (x/n) is the Jacobi symbol of x mod n. The symbol $|n|$ denotes the binary length of n.

Let Q_n be a predicate defined on Z_n^1 such that $Q_n(x)=1$ iff x is a quadratic residue mod n. Let H_k denote the set of "hard composite integers", i.e., $H_k=\{n \mid n=pq$, where p and q are distinct primes such that $|p|=|q|=k.\}$.

The security of our scheme is based on the quadratic residuosity assumption (QRA). From QRA Goldwasser and Micali have proven the following.

Lemma 1 ([1]). Under QRA, the predicate Q_n defined on Z_n^1 is unappoximable by any circuit of polynomial size even if some quadratic nonresidue mod n are known. (Recall that a circuit C ε-approximates a predicate $Q:B \rightarrow \{0,1\}$ if $C(x)=Q(x)$ for at least a fraction $1/2+\varepsilon$ of the $x \in B$.)

Let $J_n=\{x \mid 1 \leq x < n/2$ and $(x/n)=1\}$. Let QR_n denote the set of quadratic residues mod n. It is easy to prove the following

Lemma 2. Let n=pq where p and q are distinct primes such that p=q=3 mod 4. Then each $z \in QR_n$ has exactly one square root that is in J_n and we denote this root by sqr(z).

We point out that Lemma 1 will still hold when Q_n defined on Z_n^1 is restricted to J_n, and we still call the result Lemma 1.

3. The New Encryption Scheme

Let n=pq as in Lemma 2. Let y be a quadratic nonresidue mod n. Now we introduce a function E_n as follows:

$$E_n: J_n \times \{0,1\} \longrightarrow J_n \times \{0,1\}$$

$$E_n(x,0) = (x^2 \bmod n,\ 0) \quad \text{if } x^2 \bmod n < n/2,$$
$$= (-x^2 \bmod n,\ 1) \quad \text{otherwise.}$$

$$E_n(x,1) = (x^2 y \bmod n,\ 0) \quad \text{if } x^2 y \bmod n < n/2,$$
$$= (-x^2 y \bmod n,\ 1) \quad \text{otherwise.}$$

From Lemma 2 we know that E_n is invertible. The inverse of E_n is denoted by D_n and can be specified as follows:

$$D_n: J_n \times \{0,1\} \to J_n \times \{0,1\}$$

$$D_n(z,j) = (\mathrm{sqr}(z), 0) \quad \text{if } j=0 \text{ and } z \notin QR.$$

$$= (\mathrm{sqr}(zy^{-1}), 1) \quad \text{if } j=1 \text{ and } z \notin QR.$$

$$= (\mathrm{sqr}(-zy^{-1}), 1) \quad \text{if } j=1 \text{ and } z \notin QR.$$

$$= (\mathrm{sqr}(-z), 0) \quad \text{if } j=1 \text{ and } z \notin QR.$$

For convenience we denote the first and second components of $E_n(x,i)$ by $E_n^1(x,i)$ and $E_n^2(x,i)$ respectively.

For any positive integer l, E_n can be generalized as follows:

$$E_n: J_n \times \{0,1\}^l \to J_n \times \{0,1\}^l$$

$$E_n(x, m_1 \ldots m_l) = (x_l, b_1 \ldots b_l)$$

where

$$x_0 = x,$$
$$x_i = E_n^1(x_{i-1}, m_i),$$
$$b_i = E_n(x_{i-1}, m_i),$$
$$i = 1,2,\ldots,l.$$

The generalized E_n is also invertible and it's inverse is still denoted by D_n.

Now let k (an even number) be the security parameter. The new probabilistic public key cryptosystem works as follows:

(1) it randomly selects two distinct primes p and q such that $p=q=3 \bmod 4$ and $|p|=|q|=k/2$,

(2) sets $n=pq$,

(3) picks y, a quadratic nonresidue mod n, and finally,

(4) outputs $\{n,y\}$ and $\{p,q\}$.

Some user, say A, publicizes the pair $\{n, y\}$ and keeps secret the pair $\{p,q\}$.

Encryption: Suppose some user B want to send a binary message $m=m_1 \ldots m_l$ to user A. Then he encrypts m as follows:

(1) Randomly selects an $x \in J_n$ and sets $z=x$.

(2) Performs step (3) for $i=1,2,\ldots,l$.

(3) $(z,b_i) := E_n(z,m_i)$.

(4) Sends A the ciphertext $E_n(x,m)=(z,b_1 \ldots b_l)$.

Encrypting an l-bit long message m takes $O(lk^2)$ time, and m is transformed into an $(l+k-1)$-bit long ciphertext. So the message expansion is $1+(k-1)/l$ which is much less than k (the message expansion of Goldwasser and Micali's scheme).

Decryption: Upon receiving the ciphertext $(z,b_1 \ldots b_l)$, user A decrypts it as follows:

(1) Performs step (2) for $i=l,l-1,\ldots,1$.

(2) $(z,m_i) := D_n(z,b_i)$.

(3) Gets the message $m=m_1 \ldots m_l$.

Recovering m ($|m|=l$) from it's ciphertext takes $O(lk^3)$ time.

Using the proof techniques in [3] and [6], we can prove the following

Theorem. The cryptosystem introduced above is polynomially secure.

Proof. The proof is tedious long and omitted here.

4. Applications

To sign a message m, we randomly select an $x \in J_n$ and forms

$$S(m) = (m, D_n(x,m))$$

S(m) will be the signature of m. Of course this simple signature is not strong. By computing $E_n(z,b)=(x,m)$, the forger can easily forge the signature of an (unpredictable) message m. This is the so-called "chosen signature attack" and can be prevented in several ways.One way is as follows: randomly select $x,y \in J_n$, $x \neq y$, and let $S(m)=(m, D_n(x,m), D_n(y,m))$. This time forging the signature of even an unpredictable message m requires finding $w,z \in J_n$, $b,b' \in \{0,1\}^*$, such that $E_n(w,b)=E_n(z,b')$, and this seems impossible.

Note that in the above mentioned signature scheme, the signature of $m_1 \cdots m_i$ or $m_i \cdots m_1$ for any i ($1 \leq i \leq 1$) can be easily obtained when the signature of $m_1 \cdots m_1$ is known. But we may avoid this danger by letting, for example,

$$S(m_1 \cdots m_1)=(m_1 \cdots m_1, D_n(x,m_1 \cdots m_1), D_n(y, m_{l/2} \cdots m_1 \; m_1 \cdots m_{l/2+1}) .$$

Clearly various signature schemes can be devised based on our new public key cryptosystem. We leave the open problem of implementing a concrete signature scheme, together with a rigorious security proof.

References

[1] S.Goldwasser and S.Micali, Probabilistic encryption, Journal of Computer and System Sciences 28 (1984), 270-299.

[2] A.Yao, Theory and application of trapdoor functions, Proceedings of the 23rd Annual Symposium on Foundations of Computer Sciencn, 1982, 80-91.

[3] S.Micali, C.Rackoff, and B.Sloan, The notion of security for probabilistic cryptosystems, CRYPTO 86,31.

[4] R.Rivest, A.Shamir, and L.Adleman, A method for obtaining digital signatures and public key cryptosystems, Comm. ACM, 21 (1978), 120-126.

[5] M.Blum and S.Goldwasser, An efficient probabilistic public-key encryption scheme which hides all partial information, CRYPTO 84, 289-299.

[6] L.Blum, M.Blum, and M.shub, A simple unpredictable pseudo-random number generator, SIAM J. Computing, 15:2, 1986, 364-383.