Correctness of Li's Generalization of RSA Cryptosystem

Roman Popovych

January 9, 2009

Abstract. For given $N=pq$ with p and q different odd primes and natural m Li introduced the public key cryptosystem. In the case $m=1$ the system is just the famous RSA system. We answer the Li's question about correctness of the system.

1 Introduction

For given $N=pq$ with p and q different odd primes and natural m Banghe Li introduced the public key cryptosystem [1]. In the case $m=1$ the system is just the famous RSA public key cryptosystem [2].

The cryptosystem is more secure in general [2] than RSA system.

But one has to solve a few problems connected with the introduced cryptosystem. The cryptosystem works with elements of the quotient ring $Z_N[x]/(h(x))$. To construct the system it is necessary to calculate a number $\varphi(N,h)$ of units of the ring. If polynomial $h(x)$ is special to N, then formula for $\varphi(N,h)$ is given in [1], but it is not simple to verify if $h(x)$ is special. In general formulas for $\varphi(N,h)$ are not known. For degree $m=2$ of the polynomial $h(x)$ formulas for the number $\varphi(N,h)$ are given in [1].

A question of correctness of the cryptosystem emerges even in the simplest case $m=2$. We answer positively the Li's question about correctness of the system in this case.

2 Preliminaries and notations

Z_N denotes a ring of numbers modulo N. We will use the notation $f(x)=g(x)$ (mod N, $h(x)$) to represent the equation $f(x)=g(x)$ in the quotient ring $Z_N[x]/(h(x))$.

N and Z denote the set of natural numbers and integers respectively. gcd(a,b) denotes the greatest common divisor of integers a and b. Given $r\in N$, $a\in Z$ with gcd(a,r)=1 the order of a modulo r is the smallest number k such that $a^k=1$ (mod r). It is denoted $O_r(a)$. For $r\in N$, $\varphi(r)$ is Euler's totient function giving the number of numbers less than r that are relatively prime to r. It is easy to see that $O_r(a)|\varphi(r)$ for any a, gcd(a,r)=1.

$h(x)$ is called special to N if $h(x)$ mod p is irreducible over the field Z_p and $h(x)$ mod q is irreducible over the field Z_q.

A^* denotes the group of units (invertible elements) in the ring A.

Let us denote by $Z_{N,h(x)}$ the quotient ring $Z_N[x]/(h(x))$ and by $\varphi(N,h)$ a number of elements of the group $(Z_{N,h(x)})^*$

To generate public key cryptosystem in the sense of Li one has to perform the following steps:

1) to generate big random primes p,q and calculate $N=pq$
2) to generate random polynomial $h(x)=x^m+a_1x^{m-1}\ldots+a_{m-1}x+a_m\in Z_N[x]$
3) to choose random number $e\in\{2,3,\ldots,\varphi(N,h)-2\}$ with $\gcd(e,\varphi(N,h))=1$
4) to choose such $d\in\{2,3,\ldots,\varphi(N,h)-2\}$ that $ed=1 \bmod \varphi(N,h)$

Public key of the cryptosystem is (N,h,e) and private key is d.

Encryption and decryption functions are defined in the following way:

- encryption $C=E(y)=y^e$, for any $y\in Z_{N,h(x)}$,
- decryption $D(c)=c^d=y^{ed}$.

It is clear that any message can be converted to element of $Z_N[X]/(h(X))$: a series of m elements of Z_N.

Let $N=pq$ with p and q different odd primes, $h(x)=x^2+a_1x+a_2$. When $a\neq 0 \bmod p$, let $\left(\frac{a}{p}\right)$ be the Legendre symbol. We use the following notations from [1]:

$$\Delta_p=\begin{cases}0, & \text{if } \dfrac{(N+1)^2}{4}a_1^2=a_2 \bmod p\\ \left(\dfrac{\frac{(N+1)^2}{4}a_1^2-a_2}{p}\right), & \text{otherwise}\end{cases}$$

$$\Delta_q=\begin{cases}0, & \text{if } \dfrac{(N+1)^2}{4}a_1^2=a_2 \bmod q\\ \left(\dfrac{\frac{(N+1)^2}{4}a_1^2-a_2}{q}\right), & \text{otherwise}\end{cases}$$

If polynomial $h(x)$ is special to N, then $\varphi(N,h)=(p^m-1)(q^m-1)$ (see [1]), but it is not simple to verify if $h(x)$ is special as one has to verify if $h(x)$ is irreducible over the field Z_p and over the field Z_q. In the case $m>2$ formulas for $\varphi(N,h)$ are not known.

For the case $m=2$ formulas for $\varphi(N,h)$ are given in [1]:

$$+\varphi(N,h)=\begin{cases}(p^2-1)(q^2-1), & if\ \Delta_p=\Delta_q=-1\\ (p-1)(q-1)(pq-p-q+5), & if\ \Delta_p=\Delta_q=1\\ (p-1)(q-1)(pq+p-q+1), & if\ \Delta_p=1,\Delta_q=-1\\ (p-1)(q-1)(pq-p+q+1), & if\ \Delta_p=-1,\Delta_q=1\\ (p-1)(q-1)(pq-p+3), & if\ \Delta_p=0,\Delta_q=1\\ (p-1)(q-1)(pq-q+1), & if\ \Delta_p=0,\Delta_q=-1\\ (p-1)(q-1)(pq-q+3), & if\ \Delta_p=1,\Delta_q=0\\ (p-1)(q-1)(pq+q+1), & if\ \Delta_p=-1,\Delta_q=0\\ (p-1)(q-1)(pq+2), & if\ \Delta_p=0,\Delta_q=0\end{cases}$$

3 Correctness of Li's generalization of RSA public key cryptosystem

Correctness of the Li's cryptosystem means that $y^{ed}=y$ (mod $N,h(x)$). It is clear that if $y\in(Z_{N,h(x)})^*$ then $y^{ed}=y$ (mod $N,h(x)$).

Li proved [1] that if $h(x)$ is special to N then the system is correct.

He observed that in the case $m=2$, $\Delta_p=0$ or $\Delta_q=0$ the system is not correct. If $h(x)=(x+a)^2$ mod p (this is equivalent to $\Delta_p=0$) then $y^{ed}=0$. So, $y^{ed}\neq y$ since $y\neq 0$.

Li also asked the following question.

Question. *For $h(x)=x^2+a_1x+a_2$ not special to $N=pq$ with $|\Delta_p|=|\Delta_q|=1$, $ed=1$ mod $\varphi(N,h)$, is $y^{ed}=y$ for any $y\in Z_{N,h(x)}$.*

We answer this question positively.

Note that for $m=2$ the polynomial $h(x)$ is not special to N if and only if $h(x)=(x+a)(x+b)$ modulo p or modulo q.

Proposition 3.1 *Let $h(x)=x^2+a_1x+a_2$ is not special to $N=pq$ with $|\Delta_p|=|\Delta_q|=1$, $ed=1$ mod $\varphi(N,h)$. Then $y^{ed}=y$ for any $y\in Z_{N,h(x)}$.*

Proof. The Chinese remainder theorem gives the following isomorphism:

$Z_N[x]/(h(x))\cong Z_p[x]/(h(x))\times Z_q[x]/(h(x))$.

The direct product of groups $Z_p^*\times Z_q^*$ is subgroup of the group $(Z_N[x]/(h(x)))^*$. Hence $\varphi(N)|\varphi(N,h)$.

We prove the identity $y^{ed}=y$ modulo $p,h(x)$ and modulo $q,h(x)$.

Let us consider the case modulo $p,h(x)$.

If $y\in(Z_p[x]/(h(x)))^*$ then $y\in(Z_N[x]/(h(x)))^*$ and trivially $y^{ed}=y$ mod $p,h(x)$.

Assume that $y\in Z_p[x]/(h(x))-(Z_p[x]/(h(x)))^*$. Then element y must have non-trivial greatest common divisor with $h(x)$.

If $h(x)$ is irreducible modulo p then $h(x)|y$ and $y=0$ (mod p, $h(x)$). Clearly $y^{ed}=y$ mod $p,h(x)$.

If $h(x)=(x+\mathrm{a})(x+b) \bmod p$, then $y=u(x+a)$ or $y=\mathrm{v}(x+b)$ ($u,v\in Z_p^*$).

Let us consider the case $y=u(x+a)$.We now obtain that $(x+a)^2=(a-b)(x+a) \bmod p,h(x)$. Indeed $(x+a)(x+b)=x^2+(a+b)x+ab$,
$(x+a)^2=x^2+2ax+a^2=-(a+b)x-ab+2ax+a^2=(a-b)x+a(a-b)=(a-b)(x+a)$.

So $(x+a)^t=(a-b)^{t-1}(x+a) \bmod p,h(x)$ for any natural t.

Since $\varphi(N)=(p-1)(q-1)|\varphi(N,h)|ed-1$ then $u^{ed}=u$. Since $|\Delta_p|\neq 0$ then $a\neq b \bmod p$ and by little Fermat theorem $(a-b)^{\mathrm{ed}-1}=1 \bmod p$.

Therefore $y^{ed}=u^{ed}(x+a)^{ed}= u^{ed}(a-b)^{ed-1}(x+a)=u(x+a)=y$.

Proof in the case $y=v(x+b)$ is analogous.

Proof in the case modulo $q,h(x)$ is analogous. The proof is complete.

4 Conclusion

For $h(x)=x^2+a_1x+a_2$ not special to $N=pq$ with $|\Delta_p|=|\Delta_q|=1$, $ed=1 \bmod \varphi(N,h)$, the identity $y^{ed}=y$ holds for any $y\in Z_{N,h(x)}$.

Hence, if $m=2$, $|\Delta_p|=|\Delta_q|=1$ then Li's generalization of RSA public key cryptosystem is correct.

References

[1] R.Rivest, A.Shamir, M.Adleman, A method for obtaining digital signature and public key cryptosystems, Communications of the ACM, 21 (2), 1978), 120-126.

[2] Banghe Li, *Generalizations of RSA Public Key Cryptosystem*, 2005. Available at `http://iacr.eprint/2005/285.`

Roman Popovych, Department of Computer Science and Engineering,
National University Lviv Politechnika, Bandery Str.,12, 79013, Lviv, Ukraine
E-mail: popovych@polynet.lviv.ua