Low exponent attack against elliptic curve RSA

Kaoru KUROSAWA[†] *Koji OKADA*[†] *Shigeo TSUJII* [‡]

[†] Dept. of Electrical & Electronic Eng.
Tokyo Institute of Technology
2–12–1 O-okayama, Meguro-ku, Tokyo 152, JAPAN
(kkurosaw@ss.titech.ac.jp)

[‡] Dept. of Computer Science
Chuo University
1–13–27 Kasuga, Bunkyo-ku, Tokyo 112, JAPAN

Low exponent attack against elliptic curve RSA

Abstract

Hastad showed that low exponent RSA is not secure if the same message is encrypted to several receivers. This is true even if time-stamp is used for each receiver. For example, let $e = 3$. Then if the number of receivers $= 7$, the eavesdropper can find the plaintext from the seven ciphertexts of each receiver.

This paper shows that elliptic curve RSA is not secure in the same scinario. It is shown that the KMOV scheme and Demytko's scheme are not secure if $e = 5, n \geq 2^{1024}$ and the number of receivers $= 428$. In Demytko's scheme, e can take the value of 2. In this case, this system is not secure if the number of receiver $= 11$ for $n \geq 2^{175}$.

1 Introduction

Hastad showed that low exponent RSA is not secure if the same message is encrypted to several receivers [1]. This is true even if time-stamp is used for each receiver. For example, let $e = 3$. Then if the number of receivers $= 7$, the eavesdropper can find the plaintext from the seven ciphertexts of each receiver.

On the other hand, elliptic curve RSA were proposed recently [2][3]. Low exponent attack is not known against elliptic curve RSA [2], although it is much more complicated than usual RSA.

This paper shows a low exponent attack against elliptic curve RSA. It is shown that the KMOV scheme and Demytko's scheme are not secure if $e = 5, n \geq 2^{1024}$ and the number of receivers $= 428$. In Demytko's scheme, e can take the value of 2. In this case, this system is not secure if the number of receiver $= 11$ for $n \geq 2^{175}$. (Even though, each receiver has a different times-stamp and a different elliptic curve.)

2 Elliptic curve RSA

2.1 Elliptic curve [4]

Let $p > 3$ be a prime. Suppose that

$$4a^3 + 27b^2 \neq 0 \mod p.$$

Define

$$E_p(a, b) \triangleq \{(x, y) |\ y^2 = x^3 + ax + b \bmod p,\ 0 \leq x < p,\ 0 \leq y < p\} \cup \{P_\infty\}.$$

$E_p(a,b)$ forms an Abelian group under a certain addition.

1. P_∞ serves as the identity element.
2. If $P = (x_1, y_1) \in E_p(a,b)$, $-P = (x_1, -y_1)$.
3. If $Q = (x_2, y_2) \in E_p(a,b), Q \neq -P$, then $P + Q = (x_3, y_3)$, where

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

and

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if} \quad P \neq Q \\ (3x_1^2 + a)/2y_1 & \text{if} \quad P = Q. \end{cases}$$

Lemma 2.1 *Let p be an odd prime satisfying $p = 2 \bmod 3$. Then, for $0 < b < p$, $E_p(0,b)$ is a cyclic group of order $|E_p(0,b)| = p + 1$.*

Lemma 2.2 *kP denotes k times addition of P, that is,*

$$kP \triangleq P + P + \cdots + P.$$

Let $P = (x, y)$, and $kP = (x_k, y_k)$. If $y_i \neq 0 \bmod p$, then

$$x_{2i} = \frac{(x_i^2 - a)^2 - 8bx_i}{4(x_i^3 + ax_i + b)} \mod p.$$

If $x_i \neq x_{i+1}$ and $x \neq 0$, then

$$x_{2i+1} = \frac{(a - x_i x_{i+1})^2 - 4b(x_i + x_{i+1})}{x(x_i - x_{i+1})^2} \mod p.$$

2.2 KMOV scheme [2]

This method utilizes Lemma 2.1. In other words, p and q must be a special form.

Step 0 (Key Generation) User U chooses large prime p and q such that

$$p = q = 2 \mod 3.$$

U computes the product $n = pq$ and $N_n = lcm(\sharp E_p(0,b), \sharp E_q(0,b)) = lcm(p+1, q+1)$.
U chooses an integer e which is co-prime to N_n and computes an integer d such that

$$ed = 1 \mod N_n.$$

Summarizing, U's secret key is $d, (p, q, \sharp E_p(0,b), \sharp E_q(0,b)), N_n)$, and U's public key is n, e.

Step 1 (Encryption) A plaintext $M = (m_x, m_y)$ is an integer pair, where $m_x \in Z_n, m_y \in Z_n$. Let $M = (m_x, m_y)$ be a point on the elliptic curve $E_n(0, b)$, where b is determined by m_x and m_y.

Sender A encrypts the point M by encryption function $E(\cdot)$ with the receiver's public key e and n as

$$C = E(M) = eM \quad \text{over } E_n(0, b),$$

and sends a ciphertext pair $C = (c_x, c_y)$ to a receiver B.

Step 2 (Decryption) Receiver B decrypts a point C by decryption function $D(\cdot)$ with his secret key d and public key n as

$$M = D(C) = dC \quad \text{over } E_n(0, b).$$

2.3 Demytko's RSA [3]

This method utilize Lemma 2.2. p and q can be arbitrary. Let

$$\overline{E_p(a, b)} \triangleq \{(x, y) | y^2 v = x^3 + ax + b \bmod p\} \cup \{P_\infty\}$$

where v is a fixed quadratic non-residue modulo p. Then, $\overline{E_p(a, b)}$ also forms an Abelian group.

For $\forall x \in Z_p$,

$$\begin{array}{lll} \exists y & (x, y) \in E_p(a, b) & \text{or} \\ \exists y & (x, y) \in \overline{E_p(a, b)} & \end{array}$$

Let $P = (x, y)$. we write $kP = (k * x, k * y)$. Then, $k * x$ can be computed without knowing y by using Lemma 2.2 in either case.

(Key Generation) Let p and q be large primes. Let $n = pq$. Choose a and b such that $gcd(4a^3 + 27b^2, n) = 1$, arbitrarily. Let

$$\begin{array}{lll} N_1 & \triangleq & |E_p(a, b)| \\ N_2 & \triangleq & |\overline{E_p(a, b)}| \\ N_3 & \triangleq & |E_q(a, b)| \\ N_4 & \triangleq & |\overline{E_q(a, b)}|. \end{array}$$

Choose e such that

$$gcd(e, N_1) = gcd(e, N_2) = gcd(e, N_3) = gcd(e, N_4) = 1.$$

The public key is (n, e, a, b). Let $d_1, \ldots, d_4$ be

$$\begin{aligned} ed_1 &= 1 \mod lcm(N_1, N_3) \\ ed_2 &= 1 \mod lcm(N_1, N_4) \\ ed_3 &= 1 \mod lcm(N_2, N_3) \\ ed_4 &= 1 \mod lcm(N_2, N_4). \end{aligned}$$

(Encryption) Let $x \in Z_n^+$ be a plaintext. Compute $e * x \in Z_n^+$ by using Lemma 2.2. Then the ciphertext is $c = e * x$.

(Decryption) Compute $w = c^3 + ac + b \bmod n$. Let

$$i = \begin{cases} 1 & \text{if} \quad (w/p) = (w/q) = 1 \\ 2 & \text{if} \quad (w/p) = 1, (w/q) = -1 \\ 3 & \text{if} \quad (w/p) = -1, (w/q) = 1 \\ 4 & \text{if} \quad (w/p) = (w/q) = -1. \end{cases}$$

The plaintext is obtained by computing $d_i * c$ by using Lemma 2.2.

3 Hastad's attack [1]

Let (n_i, e) be an RSA public key of user U_i $(i = 1, 2, \ldots)$, where e is common and $\{n_i\}$ are relatively prime. Hastad showed that, if e is small, broad cast encryption is not secure. Suppose that A wants to send the same message x to user $U_1, U_2, \ldots, U_k$. Let t_i be the time-stamp for U_i. She will compute and send

$$y_i = (2^{|t_i|}x + t_i)^e \mod n_i.$$

y_i is a polynomial of x with degree e. Hastad proved the following Proposition.

Proposition 3.1 *Given a set of equations* $\sum_{j=0}^{h} a_{ij}x^j = 0 \bmod n_i, i = 1, 2, \ldots, k$ *where* $x < n$ *and* $gcd(\langle a_{ij}\rangle_{j=0}^{h}, n_i) = 1$ *for all* i. *Then it is possible to recover* x *in time polynomial in* e, k *and* $\log n_i$ *if*

$$N > n^{\frac{h(h+1)}{2}}(k+h+1)^{\frac{k+h+1}{2}}2^{\frac{(k+h+1)^2}{2}}(h+1)^{(h+1)}. \tag{1}$$

As before $N = \prod_{i=1}^{k} n_i$, $n = \min n_i$, h *is the degree of the equation and* k *is the number of equations.*

This Proposition means that, if $e = 3$ and $k \geq 7$, the attacker can find x from $y_1, y_2, \ldots, y_k$.

4 Low exponent attack against elliptic curve RSA

Suppose that A wants to send the same message x to $U_1, U_2, \ldots, U_k$. Let the public key of U_i of Demytko's RSA scheme be

$$(n_i, e, a_i, b_i).$$

In the KMOV scheme, $a_i = 0$ and b_i is computed from the ciphertext. Assume that $\{n_i\}$ are relatively prime. A computes and send the ciphertexts $c_1, c_2, \ldots, c_k$.

For simplicity, we omit time-stamps in the following discussion. However, Theorem 4.1 and 4.4 hold even if time-stamps are used as in [1].

4.1 $e = 2$ (attack against Demytko)

In Demytko's scheme, e can be 2 if each N_i is odd.

Theorem 4.1 *Suppose that $n \geq 2^{175}$. In Demytko's scheme, if $e = 2$ and $k \geq 11$, then x can be found from $c_1, \ldots, c_k$ in polynomial time.*

Proof. From Lemma 2.2,

$$c_i = \frac{(x^2 - a_i)^2 - 8b_i x}{4(x^3 + a_i x + b_i)} \mod n_i.$$

Let

$$F_i(x) \triangleq 4c_i(x^3 + a_i x + b_i) - (x^2 - a_i)^2 + 8b_i x \mod n_i.$$

Then,

$$F_i(x) = 0 \mod n_i$$

and $\deg F_i(x) = 4$. In Proposition 3.1, $h = 4$. Then, $n^{\frac{h(h+1)}{2}} = n^{10}$. Further, if $k = 11$,

$$(k + h + 1)^{\frac{k+h+1}{2}} 2^{\frac{(k+h+1)^2}{2}} (h + 1)^{(h+1)} = 16^8 \cdot 2^{128} \cdot 5^5 < 2^{175}.$$

Thus, the right hand side of eq.(1)

$$< 2^{175} \cdot n^{10}.$$

Therefore, if $k = 11$ and $n \geq 2^{175}$, eq.(1) holds. Q.E.D.

4.2 $e = 3$ (attack against Demytko)

Theorem 4.2 *Suppose that $n \geq 2^{482}$. If $e = 3$ and $k \geq 61$, then x can be found from $c_1, \ldots, c_k$ in polynomial times in Demytko's scheme.*

Proof. From Lemma 2.2,

$$x_2^{(i)} = \frac{(x^2 - a_i)^2 - 8b_i x}{4(x^3 + a_i x + b_i)} \mod n_i \tag{2}$$

$$c_i = \frac{(a_i - x x_2^{(i)})^2 - 4b(x + x_2^{(i)})}{x(x - x_2^{(i)})^2} \mod n_i \tag{3}$$

By substituting eq.(2) into eq.(3), we have

$$c_i = \frac{h_i(x)}{g_i(x)} \mod n_i$$

for some polynomials $h_i(x)$ and $g_i(x)$, where $\deg h_i(x) = 10$ and $\deg g_i(x) = 9$. Let

$$F_i(x) = c_i g_i(x) - h_i(x).$$

Then $F_i(x) = 0$ and $\deg F_i(x) = 10$. In Proposition 3.1, we have $h = 10$. Then, $n^{\frac{h(h+1)}{2}} = n^{55}$. Further, if $k = 61$,

$$(k + h + 1)^{\frac{k+h+1}{2}} 2^{\frac{(k+h+1)^2}{2}} (h + 1)^{(h+1)} \leq 2^{2888} < (2^{482})^6.$$

Thus, the right hand side of eq.(1)

$$< (2^{482})^6 \cdot n^{55}.$$

Therefore, if $k = 61$ and $n \geq 2^{482}$, eq.(1) holds. Q.E.D.

After a preliminary version of this paper [5], it has turned out that this bound can be tighter [6]. Namely, $k \geq 49$.

4.3 $e = 5$ (attack against KMOV and Demytko)

Theorem 4.3 *Suppose that $n \geq 2^{723}$. If $e = 5$ and $k \geq 664$, then x can be found from $c_1, \ldots, c_k$ in polynomial times for both the KMOV scheme and Demytko's scheme.*

Proof. First, we show a proof for Demytko's scheme. By the similar argument as the case $e = 3$, we have

$$c_i = \frac{h_i(x)}{g_i(x)} \mod n_i$$

for some polynomials $h_i(x)$ and $g_i(x)$, where $\deg h_i(x) = 25$ and $\deg g_i(x) = 24$. Let

$$F_i(x) = c_i g_i(x) - h_i(x).$$

Then $F_i(x) = 0$ and $\deg F_i(x) = 25$. In Proposition 3.1, we have $h = 25$. Then, $n^{\frac{h(h+1)}{2}} = n^{325}$. Further, if $k = 664$,

$$(k+h+1)^{\frac{k+h+1}{2}} 2^{\frac{(k+h+1)^2}{2}} (h+1)^{(h+1)} \leq 2^{241630} < (2^{723})^{339}.$$

Thus, the right hand side of eq.(1)

$$< (2^{723})^{339} \cdot n^{325}.$$

Therefore, if $k = 664$ and $n \geq 2^{723}$, eq.(1) holds.

Next, we show a proof for the KMOV scheme. In the KMOV scheme, a plaintext is $M = (m_x, m_y)$ and the ciphertext is $C = (c_x, c_y)$. That is, x coordinate but also y coordinate are used for encryption. m_x is found from $\{c_x\}$ in the same way as the above discussion. We show how to find m_y.

Lemma 4.1 *Let $kP = (x_k, y_k)$. Note that $(x_{2i}, y_{2i}) = (x_i, y_i) + (x_i, y_i)$, $(x_{2i+1}, y_{2i+1}) = (x_i, y_i) + (x_{i+1}, y_{i+1})$. If $y_i \neq 0$, then*

$$y_{2i} = \frac{3x_i^2 + a}{2y_i}(x_i - x_{2i}) - y_i \mod p.$$

If $x_i \neq x_{i+1}$, then

$$y_{2i+1} = \frac{y_{i+1} - y_i}{x_{i+1} - x_i}(x_i - x_{2i+1}) - y_i \mod p.$$

Lemma 4.2

$$m_y = \frac{f(m_x, x_2, x_3, c_x) - g(m_x, x_2, x_3, c_x)}{2c_y(x_2 - m_x)(x_3 - x_2)} \mod n, \tag{4}$$

where

$$\begin{aligned} f(m_x, x_2, x_3, c_x) &= 3m_x^2(m_x - x_2)\{(m_x - x_3)(x_2 - c_x) + (m_x - x_2)(x_3 - c_x)\}, \\ g(m_x, x_2, x_3, c_x) &= 2(m_x^3 + b)\{2(m_x - x_3)(x_2 - c_x) + (m_x - x_2)(x_3 - x_2)\}. \end{aligned}$$

Proof. In the KMOV scheme, $(x_1, y_1) = (m_x, m_y), (x_5, y_5) = (c_x, c_y)$ and $a = 0$. Therefore, form Lemma 4.1,

$$y_2 = \frac{3m_x^2}{2m_y}(m_x - x_2) - m_y \mod n, \tag{5}$$

$$y_3 = \frac{y_2 - m_y}{x_2 - m_x}(m_x - x_3) - m_y \mod n. \tag{6}$$

$$c_y = \frac{y_3 - y_2}{x_3 - x_2}(x_2 - c_x) - y_2 \mod n. \tag{7}$$

By substituting eq.(5) and eq.(6) into eq.(7), and note that $m_y^2 = m_x^3 + b \mod n$, we have

$$c_y = \frac{f(m_x, x_2, x_3, c_x) - g(m_x, x_2, x_3, c_x)}{2m_y(x_2 - m_x)(x_3 - x_2)} \mod n.$$

Hence, eq.(4) holds. Q.E.D.

At this moment, we know all parameters of the right hand side of eq.(4). Therefore, we can find m_y from Lemma 4.2 Q.E.D.

Theorem 4.4 *Suppose that $n \geq 2^{1024}$. If $e = 5$ and $k \geq 428$, then x can be found from $c_1, \ldots, c_k$ in polynomial times for both the KMOV scheme and Demytko's scheme.*

Further, Theorem 4.3 can be extended to any small e.

References

[1] J. Hastad, "On using RSA with low exponent in a public key network", *Proc. of Crypto'85*, pp.403-408, 1985.

[2] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone, "New public-key schemes based on elliptic curves over the ring Z_n", *Proc. of Crypto'91*, 1991.

[3] N. Demytko, "A new elliptic curve based analogue of RSA", *Proc. of Eurocrypt'93*, pp.39-48, May 24 1993.

[4] D. M. Bressoud, "Factorization and primality testing", *Springer-Verlag*, 1989.

[5] K. Kurosawa and S. Tsujii, "Low exponent attack against elliptic curve RSA", *Technical Report of IEICE*, ISEC94-2, pp.11-17, 1994

[6] H. Kuwakado and K. Koyama, "On the security of RSA-type schemes over cubic curves against the Hastad attack", *Technical report of IEICE*, ISEC94-10, pp.23-30, 1994