The Multi-variable Modular Polynomial and its Applications to Cryptography

Tsuyoshi Takagi   Shozo Naito

NTT Software Laboratories
3-9-11 Midori-cho Musashino-shi Tokyo, 180
{ttakagi,naito}@slab.ntt.co.jp

Abstract. We prove the extension of the Håstad algorithm to the multi-variable modular polynomial. Although the Håstad attack is one of the strongest known attacks on RSA-type cryptosystems, the original Håstad attack is generally not applicable to multi-variable cryptosystems, where the plain text space (the encryption domain) is multi-variable. As an application of our extension, we attack RSA-type cryptosystems over elliptic curves and show the critical number of encrypted texts.

1 Introduction

We consider the integer polynomial computational problem: when we have several modular polynomials having the same single solution, can we find the real-valued polynomial with the solution in polynomial time?

In the one-variable case, Håstad showed an algorithm for solving the problem using LLL reduction [4]. [1]

And in the same paper, he indicated a cryptological application of the algorithm: RSA type public-key cryptosystems can be broken without knowing the secret key if one plain text is sent to several people. This Håstad attack is only applicable to one-variable equations, so it cannot be used directly to attack cryptoschemes with more than one variable.

In this paper, we show that Håstad's algorithm can be extended to polynomials with more than one variable, including the original algorithm as a special case. We can apply this new attack to RSA-type cryptoschemes whose plain text space (the domain of encryption) is multi-variable without reducing them to single-variable cryptosystems. One of the most famous two-variable cryptosystems is the cryptoscheme over elliptic curves [5]. Since the elliptic cryptoscheme can be reduced from a two-variable encryption function to a one-variable function using the defnition equation, we can apply the original Håstad attack to it [6] [7]. We show that the number of encripted texts necessary for our new attack can be reduced by comparing the number with the original Håstad attack.

[1] Recently, Coppersmith, Franklin, Patarin and Reiter reported a class of low-exponent attacks against RSA cryptoscheme [2] [3]. By the attack, the plaintexs with polynomial relation under a *single* public key can be recovered. But the attack is not applicable to the case where a single message is encrypted under *multiple* different keys discussed in this paper.

On the other hand, it is generally not known whether that all multi-variable encryption functions can be converted to one-variable ones.

Section 2 extends the Håstad attack to multi-variable cryptosystems. Section 3 applies the new attack to RSA-type cryptosystems over elliptic curves and compares the results with the original Håstad attack.

2 Extension of the Håstad attack

Theorem 1 *Consider an integer coefficient equivalent k polynomial with l variables not greater than e-th degree, such as*

$$\sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\ldots+j_l\le e} a_{i,j_1,\ldots,j_l} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \equiv 0 \pmod{n_i}, \quad i=1,2,\ldots,k \tag{1}$$

where $x_1, x_2, \ldots, x_l < n$, $n = \min n_i$. Then if the following relation holds, we can get the real-valued equation in $x_1, x_2, \ldots, x_l$ in time polynomial in e, k, and $\log n_i$.

$$N > n^f (k+g)^{\frac{k+g}{2}} 2^{\frac{(k+g)^2}{2}} g^g, \tag{2}$$

where $N = \prod_{i=1}^{k} n_i$, g is the number of different terms including the constant term, and f is the sum of the degrees in $x_1, x_2, \ldots, x_l$ through all of the different terms. The maximum numbers of f and g are

$$f = \sum_{m=1}^{e} m\, {}_{l+m-1}\mathrm{C}_m, \quad g = \sum_{m=0}^{e} {}_{l+m-1}\mathrm{C}_m \tag{3}$$

Remark 1 *For Theorem 1, in the case of one variable, it is possible to solve the real-valued equation within polynomial time [4]. In the case of more than one variable, it is an open problem to solve the multi-variable algebraic equation. Some methods for solving the generic multi-variable algebraic equation are known. One method is to calculate the Gröbner bases and another is to eliminate those equations using the resultant [1]. And we note that we can construct a real-valued multi-variable polynomial that can be solved in polynomial time.*

Remark 2 *Theorem 1 includes the original Håstad attack as a special case by restricting the number of variables to one.*

Proof: Let $u_j \equiv \delta_{ij} \pmod{n_i}$, where δ_{ij} is Kronecker's delta. And $s_1, s_2, \ldots, s_k$ are particular integers determined later. Using the Chinese remainder theorem, we obtain the following equation equivalent to equations (1).

$$0 \equiv \sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\ldots+j_l\le e} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \sum_{i=1}^{k} a_{i,j_1,\ldots,j_l} s_i u_i \tag{4}$$

$$\equiv \sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\ldots+j_l\le e} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} c_{j_1,j_2,\ldots,j_l} \pmod{N}. \tag{5}$$

In n dimensional real space $\mathbf{R}^n$, we define lattice L spanned by linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ such that

$$L = \{y \,|\, y = \sum_{i=1}^{n} a_i \mathbf{b}_i,\ a_i \in \mathbf{Z}\}.$$

From Minkowski's theorem, let the shortest norm vector including lattice L be λ_1, thus

$$\lambda_1 \leq \gamma_n^{\frac{1}{2}} (\det(L))^{\frac{1}{n}},$$

where γ_n is called Hermite's constant, which is always less than n. And from LLL algorithm, within polynomial time we can find the vector satisfying

$$||\mathbf{b}||/\lambda_1 \leq 2^{\frac{n}{2}}.$$

Therefore, for $n-$dimensional lattice L, we can find vector $\mathbf{b}$ satisfying

$$||\mathbf{b}|| \leq n^{\frac{1}{2}} 2^{\frac{n}{2}} \det(L)^{\frac{1}{n}} \tag{6}$$

within polynomial time [4].

Next, for equation (5), the ${}_{l+j-1}\mathrm{C}_j$ terms, where the sum of the degrees in $x_1, x_2, \ldots, x_l$ is j, are as follows:

$$\begin{array}{l}
x_1^0 x_2^0 x_3^0 \ldots x_{l-2}^0 x_{l-1}^0 x_l^j \\
x_1^0 x_2^0 x_3^0 \ldots x_{l-2}^0 x_{l-1}^1 x_l^{j-1} \\
x_1^0 x_2^0 x_3^0 \ldots x_{l-2}^0 x_{l-1}^2 x_l^{j-2} \\
x_1^0 x_2^0 x_3^0 \ldots x_{l-2}^1 x_{l-1}^1 x_l^{j-2} \\
\ldots \\
x_1^{j-1} x_2^1 x_3^0 \ldots x_{l-2}^0 x_{l-1}^0 x_l^0 \\
x_1^j x_2^0 x_3^0 \ldots x_{l-2}^0 x_{l-1}^0 x_l^0
\end{array}$$

Then we can get $g(= \sum_{j=0}^{e} {}_{l+j-1}\mathrm{C}_j)$ terms at most in equation (5). So we associate the following vector with each term, where the number of elements is ${}_{l+j-1}\mathrm{C}_j$ at most and the degree in $x_1, x_2, \ldots, x_l$ is j:

$$\mathbf{b}_{i,j} = (a_{i,0,0,\ldots,0,j} u_i, a_{i,0,0,\ldots,1,j-1} u_i, \ldots, a_{i,j,0,\ldots,0} u_i). \tag{7}$$

Here, we generate the following $k+g$ vectors at most, where each vector includes the above vector among its elements.

$$\begin{array}{l}
\mathbf{b}_1 = (\mathbf{b}_{1,0}, n\mathbf{b}_{1,1}, n^2\mathbf{b}_{1,2}, \ldots, n^e\mathbf{b}_{1,e}, \dfrac{N}{n_1 g}, 0, \ldots, 0) \\
\mathbf{b}_2 = (\mathbf{b}_{2,0}, n\mathbf{b}_{2,1}, n^2\mathbf{b}_{2,2}, \ldots, n^e\mathbf{b}_{2,e}, 0, \dfrac{N}{n_2 g}, \ldots, 0) \\
\ldots
\end{array}$$

$$
\begin{aligned}
\mathbf{b}_k &= (\mathbf{b}_{k,0}, n\mathbf{b}_{k,1}, n^2\mathbf{b}_{k,2}, \ldots, n^e\mathbf{b}_{k,e}, 0, 0, \ldots, \frac{N}{n_k g}) \\
\mathbf{b}_{k+1} &= (N, 0, 0, \ldots, 0, 0, 0, \ldots, 0) \\
\mathbf{b}_{k+2} &= (0, nN, 0, \ldots, 0, 0, 0, \ldots, 0) \\
&\ldots \\
\mathbf{b}_{k+g} &= (0, 0, 0, \ldots, n^e N, 0, 0, \ldots, 0)
\end{aligned}
$$

Next, we consider the $(k+g)$-dimensional lattice L that is generated by these vectors. Any point in L can be written as follows:

$$
\begin{aligned}
&\sum_{i=1}^{k+g} s_i \mathbf{b}_i \\
&= (\sum_{i=1}^{k} s_i \mathbf{b}_{i,0} + s_{k+1}N, \sum_{i=1}^{k} s_i \mathbf{b}_{i,1} + s_{k+2}nN, \ldots, \frac{Ns_1}{n_1 g}, \frac{Ns_2}{n_2 g}, \ldots, \frac{Ns_k}{n_k g}) \\
&\equiv (c_{0,0,\ldots,0,0}, nc_{0,0,\ldots,0,1}, nc_{0,0,\ldots,1,0}, \ldots, \frac{Ns_1}{n_1 g}, \frac{Ns_2}{n_2 g}, \ldots, \frac{Ns_k}{n_k g}) \, (\mathrm{mod} N),
\end{aligned}
$$

where $s_1, s_2, \ldots, s_k$ are arbitrary integers. Therefore, from equation (6), we can find vector $\mathbf{b}$ satisfying the following condition in polynomial time.

$$||\mathbf{b}|| \leq (k+g)^{\frac{1}{2}} 2^{\frac{k+g}{2}} \mathrm{Det}(L)^{\frac{1}{k+g}}$$

The following equation holds:

$$\mathrm{Det}(L) = n^f N^{k+g-1} g^{-k},$$

where $f = \sum_{j=1}^{e} j \, {}_{l+j-1}\mathrm{C}_j$. Finally we can find vector $\mathbf{b}$ satisfying the following condition within polynomial time.

$$||\mathbf{b}|| \leq (k+g)^{\frac{1}{2}} 2^{\frac{k+g}{2}} (n^f N^{k+g-1} g^{-k})^{\frac{1}{k+g}} \tag{8}$$

In equation (5), if the relation

$$|c_{j_1,j_2,\ldots,j_l}| \leq \frac{N}{g n^{j_1+j_2+\ldots+j_l}} \tag{9}$$

holds, then noticing $x_1, x_2, \ldots, x_l < n$, we obtain

$$
\begin{aligned}
&\left| \sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\ldots+j_l \leq e} x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} c_{j_1,j_2,\ldots,j_l} \right| \\
\leq &\sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\ldots+j_l \leq e} n^{j_1+j_2+\ldots+j_l} |c_{j_1,j_2,\ldots,j_l}| < N.
\end{aligned}
$$

Therefore we can obtain equation (5) as the real-valued equation. Now consider how we should get the vector $\mathbf{b}$ satisfying equation (9). If the condition

$$||\mathbf{b}|| \leq \frac{N}{g} \tag{10}$$

is satisfied, then equation (9) is also satisfied, while if the norm of the vector $\mathbf{b}$ is greater than N/g, then equation (9) is never satisfied.

Therefore, the vector satisfying both the equations (10) and (8) is the vector we are seeking, this means that

$$N > n^f (k+g)^{\frac{k+g}{2}} 2^{\frac{(k+g)^2}{2}} g^g \tag{11}$$

holds. Here, f and g are numbers associated with terms in the equation as described in the theorem.

After determining the vector $\mathbf{b}$, we can find the coefficients of the vector $\mathbf{b}$ spanned by the basis $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{K+g}$. Then the integers $s_1, s_2, \ldots, s_k$ are also determined. And it is clear that the vector we choose here is not zero. $\square$

3 Attack on RSA-type cryptoschemes over elliptic curves

3.1 RSA-type cryptoschemes

We can construct RSA-type cryptoschemes over ellilptic curves [5]. We state only the information needed for the attack. The elliptic curve over real field $\mathbf{R}$ is

$$E(a,b) := \{(x,y) \,|\, y^2 = x^3 + ax + b\} \cup P_\infty, \tag{12}$$

where P_∞ is a point at infinity; $a, b \in \mathbf{R}$; and $4a^3 + 27b^2 \neq 0$. Then, $E(a,b)$ has the structure of an abelian group. Actually, for any pair of points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, we define $P + Q = (x_3, y_3)$ as follows:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & if \quad x_1 \neq x_2 \\[2ex] \dfrac{3x_1^2 + a}{2y_1} & if \quad x_1 = x_2 \end{cases}$$

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

We can also define the same operation over the ring $\mathbf{Z}_n$.

Now, we calculate e times the value of any point $P = (x,y)$ in $E(a,b)$ i.e., $e \star P = (e \star x, e \star y)$.

From the group law, $e \star P$ is generally a rational function of x and y. So, letting $f_x(x,y), f_y(x,y), g_x(x,y), g_y(x,y)$ be polynomials in x and y, then we have

$$e \star x = \frac{g_x(x,y)}{f_x(x,y)}, \quad e \star y = \frac{g_y(x,y)}{f_y(x,y)}.$$

From these rational functions, we obtain the following two-variable polynomial equations in x and y, which are the ones theorem 1 is applicable to.

$$e \star x f_x(x, y) - g_x(x, y) = 0$$
$$e \star y f_y(x, y) - g_y(x, y) = 0$$

Furthermore, in the elliptic curve cryptosystem, by investigating the division polynomials and using the definition equation $y^2 = x^3 + ax + b$, we can reduce the above two-variable polynomials into one-variable polynomials with x as the only variable. Therefore we can also apply the original Håstad attack to the reduced one-variable polynomials. This method was first pointed out by Kurosawa-Tujii [6], and the number of polynomials necessary for the attack was accurately calculated by Kuwakado-Koyama [7]. This prominent property of the elliptic functions that $e \star x$ can be described with only x with the definition equation comes from the fact that the division polynomials of $e \star x$ are polynomials in terms of y^2.

Next, we compare the number of $e \star x$ polynomials necessary for applying the two types of attacks, that is, attacks for one- or two-variable polynomials. To apply theorem 1, we have to calculate the numbers f and g, where g is the number of different terms in the $e \star x$ polynomial including the constant term, and f is the sum of the degrees of all the different terms. In the next section, by investigating division polynomials of $e\star$ operations, we get general formulas describing f and g for one- and two-variable $e \star x$ polynomials. On the other hand, because the Håstad attack cannot work for polynomials with large e [7], we investigate f and g for ones with small e in detail.

3.2 Division polynomials

Division polynomials $\psi_e \in \mathbf{Z}[a, b, x, y]$ are inductively defined as follows:

$$\begin{aligned}
&\psi_1 = 1, \quad \psi_2 = 2y, \\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2, \\
&\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
&\psi_{2e+1} = \psi_{e+2}\psi_e^3 - \psi_{e-1}\psi_{e+1}^3 \ (e \geq 2), \\
&2y\psi_{2e} = \psi_e(\psi_{e+2}\psi_{e-1}^2 - \psi_{e-2}\psi_{e+1}^2) \ (e \geq 3).
\end{aligned}$$

It is easy to check that the ψ_{2e}'s are polynomials. We further define polynomials ϕ_e and ω_e by

$$\phi_e = x\psi_e^2 - \psi_{e+1}\psi_{e-1}$$
$$4y\omega_e = \psi_{e+2}\psi_{e-1}^2 - \psi_{e-2}\psi_{e+1}^2.$$

$\psi_e, \phi_e, y^{-1}\omega_e$ (for e odd) and $(2y)^{-1}\psi_e, \phi_e, \omega_e$ (for e even) are polynomials in $\mathbf{Z}[a, b, x, y^2]$. Hence replacing y^2 by $x^3 + ax + b$, we can treat them as polynomials in $\mathbf{Z}[a, b, x]$.

As polynomials in x, we can show that

$$\phi_e(x) = x^{e^2} + lower\ order\ terms$$
$$\psi_e(x)^2 = e^2 x^{e^2-1} + lower\ order\ terms.$$

Let $P = (x, y) \in E(a, b)$. Then using these polynomials, we can describe $e \star P$ as follows:

$$e \star P = \left(\frac{\phi_e(P)}{\psi_e(P)^2}, \frac{\omega_e(P)}{\psi_e(P)^3} \right).$$

Therefore we obtain the following theorem describing f and g in one-variable $e \star x$ polynomials. (See, for example, [8])

Here, we investigate the number and degree of the different terms corresponding to the changes of e. Then we have the next lemma.

Lemma 1 *Let $f_1(e)$ be the sum of the degrees of all different terms and $g_1(e)$ be the number of different terms including a constant term in $e \star x$ one-variable polynomials. Then the following holds:*

$$f_1 = \frac{e^2(e^2+1)}{2} \tag{13}$$
$$g_1 = e^2 + 1 \tag{14}$$

On the other hand, replacing x^3 by $y^2 - ax - b$, we can treat division polynomials with not more than two degrees for variable x. In this treatment, division polynomials ψ_k are inductively defined as follows:

$$\begin{aligned}
&\psi_1 = 1, \quad \psi_2 = 2y,\\
&\psi_3 = 3xy^2 + 3ax^2 + 9bx - a^2,\\
&\psi_4 = 4y(y^4 + 3axy^2 + 18by^2 - 9a^2x^2 - 27abx - 27b^2 - a^3),\\
&\psi_{2e+1} = \psi_{e+2}\psi_e^3 - \psi_{e-1}\psi_{e+1}^3 (e \geq 2),\\
&2y\psi_{2e} = \psi_e(\psi_{e+2}\psi_{e-1}^2 - \psi_{e-2}\psi_{e+1}^2)(e \geq 3).
\end{aligned}$$

From these polynomials, it is easy to obtain the following theorem.

Theorem 2 *Let $f_2(e)$ be the sum of the degree of all different terms and $g_2(e)$ be the number of different terms including a constant term in $e \star x$ two-variable polynomials. Then the following holds:*

$$f_2 = \begin{cases} 3l^2 + 2l & if\ e = 0\ mod\ 3 \\ 3l^2 + 4l + 1 & otherwise \end{cases} \tag{15}$$
$$g_2 = e^2 + 1, \tag{16}$$

where $l = \lfloor \frac{e^2}{3} \rfloor$.

We note that g_1 in lemma 1 and g_2 in theorem 2 have the same value. For f_1 and f_2, the difference is calculated as follows:

$$f_1 - f_2 = \begin{cases} \dfrac{3l^2 - l}{2} & \text{if } e = 0 \ mod\ 3 \\ \dfrac{3l^2 + l}{2} & \text{otherwise} \end{cases} \tag{17}$$

From this equation, we find that f_2 is always smaller than f_1, and the difference increases with the square of l.

Next, let e be the exponent of the encryption. And when lemma 1 and theorem 2 are applied to encryption function, we obtain the following f_1, g_1, f_2, and g_2 table for small exponent e.

exponent e	2	3	4	5	6	7
one variable: g_1, f_1	5, 10	10, 45	17, 136	26, 338	37, 703	50, 1408
two variable: g_2, f_2	5, 8	10, 32	17, 96	26, 225	37, 456	50, 833

Table 1. f and g values of one- and two-variable polynomials

3.3 Attacks to the cryptosystem

Using the f and g values obtained in the above section, we can calculate the number of $e \star x$ polynomials necessary to obtain a real-valued equation. The numbers are listed in Tables 2 and 3 for 512-bit and 1024-bit encryption keys respectively. From these tables, we can observe that the number of two variables is always smaller than the number of one variables, and the difference increases as the exponent of e increases. Here, we have a question: Is the real-valued two-

exponent e	2	3	4	5	6	$7 \geq$
one-variable	11	49	173	*	*	*
two-variable	9	36	114	464	*	*

Table 2. Number of polynomials (512-bit means)

variable polynomial solvable? The answer is affirmative, because $e \star x$ polynomials of two variables are polynomials in $\mathbf{Z}[a, b, x, y^2]$, so if we replace y^2 by $x^3 + ax + b$, we can treat them as polynomials in $\mathbf{Z}[a, b, x]$. After this treatment, we can apply

the exponent e	2	3	4	5	6	$7 \geq$
one-variable	11	47	151	428	*	*
two-variable	9	35	104	269	814	*

Table 3. Number of polynomials (1024-bit means)

the LLL algorithm to the real-valued polynomial in one variable of x. Therefore, we can recover the plain text. From this discussion, theorem 1 means that the two-variable attack is stronger than the original one-variable Håstad attack.

Theorem 3 *The RSA-type cryptoscheme with low exponent e over the elliptic curve is not secure when sending a number of messages encrypting the same plaintext equal to or greater than the number listed in tables 3.*

4 Conclusion

We extended the Håstad attack to multi-variable polynomial1 and applied this new attack to RSA-type cryptosystems over elliptic curves. This new attack is stronger than the original attack, which is applied to the one-variable polynomials obtained by using the definition polynomial of the elliptic curve.

References

1. B. Buchberger, "Application of gröbner bases in non-linear computer science," Lecture Notes in Computer Science, Vol.296, (1987), pp.52–80.
2. D. Coppersmith, M. Franklin, J. Patarin, M. Reiter, "Low-exponet RSA with related messages," Advances in Cryptology – EUROCRYPT '96, LNCS 1070, (1996), pp.1–9.
3. D. Coppersmith, "Finding a small root of a univariate modular equation," Advances in Cryptology – EUROCRYPT '96, LNCS 1070, (1996), pp.155-165.
4. J. Håstad, "Solving simultaneous modular equations of low degree," SIAM J. Computing, Vol.17, No.2, (1988), pp.336-341.
5. K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone, "New public-key schemes based on elliptic curves over the ring $\mathbf{Z}_n$," Advances in Cryptology – CRYPTO '91, LNCS 576, (1992), pp.252-266.
6. K. Kurosawa, K. Okada, S. Tsujii, "Low exponent attack against elliptic curve RSA," Information Processing Letters, 53, (1995), pp.77-83.
7. H. Kuwakado, K. Koyama; "Security of RSA-type cryptosystems over elliptic curves against the Håstad attack," Electronics Letters, 30, No.22, (1994), pp.1843-1844.
8. J. H. Silverman, "The arithmetic of elliptic curves," GTM106, Springer-Verlag, Berlin, 1986.

This article was processed using the LaTeX macro package with LLNCS style