UCL Crypto Group Technical Report Series

Takagi/Naito's algorithm revisited

M. Joye, F. Koeune and J.-J. Quisquater

http://www.dice.ucl.ac.be/crypto/

Technical Report
CG–1997/3.2

Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium

Phone: (+32) 10 472541
Fax: (+32) 10 472598

Takagi/Naito's algorithm revisited

M. Joye[1)], F. Koeune[2)] and J.-J. Quisquater[2)]

March 29,1997

[1)] Département de Mathématique (AGEL), Université catholique de Louvain
Chemin du Cyclotron, 2, B-1348 Louvain-la-Neuve, Belgium
E-mail: `joye@agel.ucl.ac.be`

[2)] Département d'Électricité (DICE), Université catholique de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
E-mail: `{fkoeune,jjq}@dice.ucl.ac.be`

Abstract. Recently, Takagi and Naito extended the Håstad algorithm to the multivariate case. In this report, we simplify the proof of their theorem. We also significantly improve their bound.

1 Introduction

In [2], Håstad presented a way to solve a system of univariate modular polynomial equations. His method was based on the use of LLL to reduce a lattice of dimension $k+e+1$, where k is the number of equations and e is the maximal degree of the polynomial equations. After publication, Rivest suggested a great simplification of the proof, reducing the lattice dimension to $e+2$ and yielding a significant improvement of some bound (see below for more details). This improved version was published in [3].

Recently, Takagi and Naito [4] extended the initial Håstad algorithm to the multivariate case. We will show that the same improvement as Rivest suggested can be applied to the extended algorithm, resulting in the same proof simplification and bound improvement.

2 Improvement

The theorem we are going to prove is the following.

CG–1997/3.2

Theorem 1. *Consider the system of k modular polynomial equations of degree $\leq e$ with l variables*

$$\sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\cdots+j_l\leq e} a_{i,j_1,\ldots,j_l}\, x_1^{j_1} x_2^{j_2}\ldots x_l^{j_l} \equiv 0 \pmod{n_i} \quad \textit{for } i=1,2,\ldots,k \qquad (1)$$

where $x_1,\ldots,x_l < n$ and $n = \min n_i$.
Suppose that the moduli n_i are coprime and that

$$\gcd(\langle a_{i,j_1,j_2,\ldots,j_l}\rangle_{j_1+j_2+\ldots+j_l=0}^{j_1+j_2+\ldots+j_l\leq e}, n_i) = 1 \quad (\forall 1\leq i\leq k)$$

* *Let g be the (max.) number of different terms, f be the (max.) sum of the degrees in $x_1,x_2,\ldots,x_l$ through all of the different terms†, and $N=\prod_{i=1}^k n_i$. If $N > n^f 2^{\frac{g(g+1)}{4}} g^g$, then we can get in polynomial time a real-valued equation which is equivalent to (1).*

Remarks. 1) This bound has to be compared with Takagi-Naito's bound, i.e.

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

2) Theorem 1 includes the improved Håstad attack as a special case by reducing the number of variables to one.

Our proof will be based on the following simple lemma.

Lemma 2. *The polynomial modular equation*

$$\sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\cdots+j_l\leq e} c_{j_1,j_2,\ldots,j_l}\, x_1^{j_1} x_2^{j_2}\ldots x_l^{j_l} \equiv 0 \pmod{N} \qquad (2)$$

is equivalent to its real-valued corresponding if

$$|c_{j_1,j_2,\ldots,j_l}| \leq \frac{N}{g\, n^{j_1+j_2+\cdots+j_l}} \quad (\forall j_1,j_2,\ldots,j_l). \qquad (3)$$

*By this notation, we mean that the greatest common divisor of n_i and all $a_{i,j_1,\ldots,j_l}$ is equal to 1.

†One can easily show that

$$f=\sum_{m=1}^{e} m\binom{m+l-1}{m} \quad \text{and} \quad g=\sum_{m=0}^{e}\binom{l+m-1}{m}.$$

Proof. Since $x_1, x_2, \ldots, x_l < n$, we have

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

Therefore, we can simply consider Eq. (2) as a real-valued equation. □

Proof (Theorem 1). Let $u_j = \delta_{ij} \pmod{n_i}$, where δ_{ij} is Kronecker's delta.
Using the Chinese remainder theorem, we obtain

$$\begin{aligned}0 &\equiv \sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\cdots+j_l\le e} \left(\sum_{i=1}^{k} a_{i,j_1,j_2,\ldots,j_l} u_i\right) x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \\ &\equiv \sum_{j_1,j_2,\ldots,j_l=0}^{j_1+j_2+\cdots+j_l\le e} c_{j_1,j_2,\ldots,j_l}\, x_1^{j_1} x_2^{j_2} \ldots x_l^{j_l} \pmod{N},\end{aligned} \tag{4}$$

which is equivalent to Eq. (1).

The idea is to multiply Eq. (4) by a constant factor in order to meet the conditions of Lemma 2. Therefore, we will consider a lattice L whose basis is given by

$$\begin{array}{lcl}\vec{\mathbf{b_1}} &=& (c_{0,\ldots,0}, nc_{0,\ldots,0,1}, nc_{0,\ldots,0,1,0}, \ldots, n^{j_1+j_2+\cdots+j_l} c_{j_1,j_2,\ldots,j_l}, \ldots, n^e c_{e,0,\ldots,0}, \frac{1}{g}) \\ \vec{\mathbf{b_2}} &=& (N, 0, 0, \ldots, 0, \ldots, 0, 0) \\ \vec{\mathbf{b_3}} &=& (0, nN, 0, \ldots, 0, \ldots, 0, 0) \\ \vec{\mathbf{b_4}} &=& (0, 0, nN, \ldots, 0, \ldots, 0, 0) \\ &\vdots& \\ \vec{\mathbf{b_{i+1}}} &=& (0, 0, 0, \ldots, n^{j_1+j_2+\cdots+j_l} N, \ldots, 0, 0) \\ &\vdots& \\ \vec{\mathbf{b_{g+1}}} &=& (0, 0, 0, \ldots, 0, \ldots, n^e N, 0)\end{array}$$

A vector of this lattice is of the form $\vec{\mathbf{V}} = S\vec{b_1} + \sum_{i=1}^{g} s_i \vec{b_{i+1}}$. Its ith coordinate (apart from the last one) is given by

$$V_i = n^{j_1+\cdots+j_l}(Sc_{j_1,\ldots,j_l} + s_i N).$$

Suppose that we find a vector $\vec{\mathbf{V}}$ such that $\|\vec{\mathbf{V}}\| < N/g$, then $|V_i| < N/g$. So,

$$\left|\frac{V_i}{n^{j_1+\cdots+j_l}}\right| = \left|\frac{V_i}{n^{j_1+\cdots+j_l}} \bmod_{\pm} N\right| = |Sc_{j_1,\ldots,j_l} \bmod_{\pm} N| < \frac{N}{g\, n^{j_1+\cdots+j_l}},$$

for all $j_1, \dots, j_l$†. S would thus be an appropriate constant for our purpose.

So, all we have to do is to find a sufficiently small vector $\vec{\mathbf{V}}$. As proved in [1, pp. 84-85], we can, using the LLL algorithm, find within polynomial time a vector $\vec{\mathbf{V}}$ such that

$$\|\vec{\mathbf{V}}\| \leq 2^{g/4} (\det L)^{1/(g+1)}.$$

Therefore, LLL will provide us the required vector $\vec{\mathbf{V}}$ if

$$2^{g/4} \left(\frac{N^g n^f}{g}\right)^{1/(g+1)} < \frac{N}{g} \iff 2^{g(g+1)/4} g^g n^f < N,$$

which is the announced condition.

To finish the proof, we must now show that the equation we obtain, namely

$$\sum_{j_1, j_2, \dots, j_l = 0}^{j_1 + j_2 + \cdots + j_l \leq e} S c_{j_1, j_2, \dots, j_l} x_1^{j_1} x_2^{j_2} \dots x_l^{j_l} \equiv 0 \pmod{N} \tag{5}$$

is non-trivial.

First note that the last coefficient of $\vec{\mathbf{V}}$ is equal to S/g, and therefore $|S| < N$, since $\|\vec{\mathbf{V}}\| < N/g$. Note also that $S \neq 0$, because all nonzero vectors $\vec{\mathbf{V}}$ with $S = 0$ are of length at least N. So, $0 < |S| < N$, whence $S \not\equiv 0 \pmod{N}$, and thus $S \not\equiv 0 \pmod{n_i}$ for some i. Furthermore, since $c_{j_1, j_2, \dots, j_l} \equiv a_{i, j_1, j_2, \dots, j_l} \pmod{n_i}$ and $\gcd(a_{i, j_1, j_2, \dots, j_l}, n_i) = 1$ for at least one $(j_1, j_2, \dots, j_l)$, there exists at least one $c_{j_1, j_2, \dots, j_l} \not\equiv 0 \pmod{n_i}$. Consequently, Eq. (5) is nontrivial and the proof is complete. □

References

[1] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 1993.

[2] Johan Håstad, *On using RSA with low exponent in a public key network*, Advances in Cryptology – Crypto '85 (H. C. Williams, ed.), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, 1986, pp. 404–408.

[3] Johan Håstad, *Solving simultaneous modular equations of low degree*, SIAM J. Comput. **17** (1988), no. 2, 336–341.

†The notation $a = b \bmod_{\pm} N$ means that a is the unique integer congruent to b modulo N such that $-\lceil N/2 \rceil + 1 \leq a \leq \lfloor N/2 \rfloor$.

[4] Tsuyoshi Takagi and Shozo Naito, *The multi-variable modular polynomial and its applications to cryptography*, 7th International Symposium on Algorithm and Computation, ISAAC'96, Lecture Notes in Computer Science, vol. 1178, Springer-Verlag, 1996, pp. 386–396.