# HOW TO BREAK OKAMOTO'S CRYPTOSYSTEM BY REDUCING LATTICE BASES

Brigitte VALLÉE[1)] Marc GIRAULT[2)] Philippe TOFFIN[1)]

[1)]Département de Mathématiques
Université 14032 Caen Cedex, France

[2)]Service d'Etudes communes des Postes et Télécommunications
BP 6243 14066 Caen Cedex, France

## ABSTRACT

The security of several signature schemes and cryptosystems, essentially proposed by Okamoto, is based on the difficulty of solving polynomial equations or inequations modulo $n$. The encryption and the decryption of these schemes are very simple when the factorisation of the modulus, a large composite number, is known.

We show here that we can, for any odd $n$, solve, in polynomial probabilistic time, quadratic equations modulo $n$, even if the factorisation of $n$ is hidden, provided we are given a sufficiently good approximation of the solutions. We thus deduce how to break Okamoto's second degree cryptosystem and we extend, in this way, Brickell's and Shamir's previous attacks.

Our main tool is lattices that we use after a linearisation of the problem, and the success of our method depends on the geometrical regularity of a particular kind of lattices.

Our paper is organized as follows:

First we recall the problems already posed, their partial solutions and describe how our results solve extensions of these problems. We then introduce our main tool, lattices and show how their geometrical properties fit in our subject. Finally, we deduce our results. These methods can be generalized to higher dimensions.

---

This work was supported in part by PRC *Mathématiques et Informatique* and in part by a convention between SEPT and University of Caen.

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 281-291, 1988.

# I. INTRODUCTION

In this section, after some definitions, we describe the problems posed by the security of Okamoto schemes, and the partial solutions given by Brickell and Shamir. Then, we state our main results and show how they extend the previous ones.

## I.1. Definitions and notations

For an odd integer $n$, $Z(n)$ denotes the ring of the integers modulo $n$ which is identified with $[0, n-1]$.

We will use approximations of a number $x_0$ in $Z(n)$. So, we adopt the following definitions and notations:

$|u|$ denotes, for $u \in Z(n)$, the minimum of $u$ and $n-u$,

$I(a, x_0)$ denotes the set of $x \in Z(n)$ such that $x = x_0 + u$, $|u| \leq n^a$,

$J(a, x_0)$ denotes the set of $x \in Z(n)$ such that

$$x = u_1 x_0 + u_2, \quad |u_1| \leq n^{a/2}, \quad |u_2| \leq n^{a/2}.$$

The subsets $I(a, x_0)$ –resp $J(a, x_0)$– and $I(b, y_0)$ are said *compatible* if there exists $x$ in $I(a, x_0)$ –resp $J(a, x_0)$– and $y$ in $I(b, y_0)$ such that $y \equiv x^2$ $[n]$.

## I.2. Okamoto's cryptographic proposals and questions

In this section, the modulus $n$ is particular: $n = p^2 q$ where $p$ and $q$ are distinct primes ($p < q$). An element $x_0$ of $Z(n)$ is called *easy* when it is smaller than $(1/2)\sqrt{pq}$ modulo $pq$.

The following cryptographic schemes are based on the difficulty of extracting square roots modulo $n$, when the factors of $n$ are unknown:

### Cryptosystems

In [6], Okamoto proposed a first public key cryptosystem:

The public key is the pair $(n, x_0)$, where $x_0$ is an easy element of $Z(n)$. From a message $u$, which is small compared to $n$, the cipher text $y$ is built as follows:

$$y \equiv (x_0 + u)^2 \quad [n]$$

As quoted in [7], Shamir [8] has two attacks to break this system: the first one works for any pair $(n, x_0)$ while the second one uses the particular form of the public key.

Okamoto [7] then proposed a new cryptosystem: $x_0$ is the known quotient modulo $n$ of two secret easy numbers of $Z(n)$. A message $(u_1, u_2)$, where the $u_i$'s are small compared to $n$, gives a cipher text $y$ such that

$$y \equiv (u_1 x_0 + u_2)^2 \quad [n].$$

Okamoto stated as an open question the breaking of this second system.

We show here that *we can break this new cryptosystem* without using the particular form of the public key $(n, x_0)$.

### Signature Scheme

In [5], Okamoto and Shiraishi proposed a signature scheme:

Given a 'one-way' function $h$, a signature $x$ is considered as valid for a message $u$ if

$$h(u) \leq (x^2 \bmod n) \leq h(u) + O(n^{2/3}) \quad \text{with } |x| \text{ not 'too small'}.$$

Brickell [2] broke this scheme, without using the particular form of $n$.

Now, we state and solve problems which are natural extensions of all the questions that we described above.

## I.3. Two Problems

### Problem 1.

*Given a square $y_0$ and a subset $I(a, x_0)$ (resp $J(a, x_0)$) which is known to contain a square root $x$ of $y_0$, find $x$.*

### Problem 2.

*Given $I(b, y_0)$ a subset of $Z(n)$, find $x$ such that $x^2$ belongs to $I(b, y_0)$.*

Solving the first problem with the intervals $I$ breaks the first version of Okamoto's cryptosystem, while the second version of Okamoto's cryptosystem is attacked by solving this problem with the subsets $J$. The second problem is linked with improvements of Brickell's results.

## I.4. Our main results: Three theorems

We state here our main results which solve generalisations of each of the problems. On the one hand, Theorem 1 and Theorem 1bis, which are uniqueness results, allow us to break the second version of Okamoto's cryptosystems, but also to make precise some points of Shamir's attack on the first version. On the other hand, Theorem 2, which is an existence result, improves Brickell's previous attack of the signature scheme.

### THEOREM 1.

*For any $n, \epsilon > 0, a$ and $b$ reals in $[0,1]$ satisfying*

$$2a + b = 1 - 3\epsilon \text{ and } b \geq a,$$

*there exists an exceptional subset $T(\epsilon)$ of $Z(n)$ such that the following is true:*

*i) Card $T(\epsilon) \leq n^{1-\epsilon}$*

*ii) For any $x_0$, not in $T(\epsilon)$ and any $y_0$ in $Z(n)$, intervals $J(a,\ x_0)$ and $I(b,\ y_0)$ have at most two compatible pairs, say $(x,y)$ and $(n-x,y)$.*

*Moreover, there exists a probabilistic polynomial algorithm A which provides one of the following three answers:*

*'exceptional case' if $x_0$ is in $T(\epsilon)$*

*'no compatible couple'*

*$(x,y)$ and $(n-x,y)$ are the two compatible pairs.*

### THEOREM 1 BIS.

*For any $n, \epsilon > 0, a$ and $b$ reals in $[0,1]$ satisfying*

$$a + b = 1 - 2\epsilon \text{ and } b \geq 2a,$$

*there exists an exceptional subset $T'(\epsilon)$ of $Z(n)$ such that the following is true:*

*i) Card $T'(\epsilon) \leq n^{1-\epsilon}$*

*ii) For any $x_0$, not in $T'(\epsilon)$ and any $y_0$ in $Z(n)$, intervals $I(a,\ x_0)$ and $I(b,\ y_0)$, have at most one compatible pair.*

*Moreover, there exists a probabilistic polynomial algorithm B which provides one of the following three answers:*

*'exceptional case' if $x_0$ is in $T'(\epsilon)$*

*'no compatible couple'*

*$(x, y)$ is the only compatible pair.*

**THEOREM 2.**

*For any $n, \epsilon > 0, a$ and $b$ reals in $[0, 1]$ satisfying*

$$a + b = 1 + 2\epsilon \text{ and } b \geq 2a,$$

*there exists an exceptional subset $T"(\epsilon)$ of $Z(n)$, such that the following is true:*

*i) Card $T"(\epsilon) \leq n^{1-\epsilon}$*

*ii) For any $x_0$, not in $T"(\epsilon)$ and for any $y_0$ in $Z(n)$, intervals $I(a, x_0)$ and $I(b, y_0)$ are compatible.*

*Moreover, there exists a probabilistic polynomial algorithm C which provides one of the following answers:*

*'exceptional case' if $x_0$ is in $T"(\epsilon)$*

*a compatible pair $(x, y)$ otherwise.*

We give now the proofs of our results, mainly for Theorem 1, in the case of subsets $J$, and see how our methods work for the intervals $I$, in the proof of theorems 1bis and 2. The main tool is *lattices* for which there are two basic facts:

a) There is a high proportion of lattices with given determinant having their smallest vector *not* too small.

b) Given a lattice and a point $m$ in the space, one can find -using an algorithm based on LLL reduction algorithm [4]- one point $t$ which belongs to the lattice and which is close to $m$.

## II. THE BREAKING OF OKAMOTO'S CRYPTOSYSTEM: proof of Theorem 1

Given $n, x_0, y_0, a, b$, we must find $u_1$ and $u_2$ that satisfy

$$|u_1| \leq n^{a/2} \quad , \quad |u_2| \leq n^{a/2} \quad , \quad |v| \leq n^b \tag{1}$$

and that are solutions of the equation

$$(u_1 x_0 + u_2)^2 \equiv y_0 + v \ [n]$$

## II.1. How lattices are involved

We must solve

$$u_1^2 x_0^2 + 2x_0 u_1 u_2 + u_2^2 - v \equiv y_0 \ [n] \tag{2}$$

Replacing $u_1^2$, $u_1 u_2$, $v - u_2^2$ by independent variables, we consider a first lattice:

$$L(x_0) := \{ w = (w_0, w_1, w_2) \in \mathbf{Z}^3 \ ; \ x_0^2 w_0 + 2x_0 w_1 - w_2 \equiv 0 \ [n] \}$$

$L(x_0)$ is spanned by the three column vectors of the matrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ x_0^2 & 2x_0 & n \end{pmatrix} \quad \text{which has determinant } n.$$

Since $|u_1|, |u_2|, |v|$ are small, we have to look for $w$ in $L(x_0)$ with the following approximations:

$$|w_0| \leq n^a, \quad |w_1| \leq n^a, \quad |w_2 - y_0| \leq 2n^b \quad (a \leq b)$$

These approximations are not of the same order, and since we will work with the norm sup, it is natural to consider a second lattice $M(x_0)$.

If $k_0, k_1, k_2$ are three positive rationals, whose product is equal to 1, we define

$$M(x_0) := \{ t \in \mathbf{Q}^3 \ ; \ t_i = k_i w_i, \ 0 \leq i \leq 2 \ \text{ and } \ w \in L(x_0) \}.$$

$M(x_0)$ has then for matrix

$$\begin{pmatrix} k_0 & 0 & 0 \\ 0 & k_1 & 0 \\ k_2 x_0^2 & 2k_2 x_0 & k_2 n \end{pmatrix} \quad \text{which has still determinant } n.$$

With a suitable choice of $(k_0, k_1, k_2)$, we get the same approximation order on each component. So, we have to find a point $t$ in $M(x_0)$ which is close to the point $m = (0, 0, k_2 y_0)$ for the norm sup.

Now, we are lead to some important questions:

1) *How to get, in a given lattice $M$ of $\mathbf{Q}^3$ a point $t$ close to a given point $m$ ?*
2) *How to be sure that such a point will be unique ?*

We answer now these two questions.

## II.2. The ClosePoint Algorithm

We get a reduced basis $\alpha = (\alpha_0, \alpha_1, \alpha_2)$ of $M$ by using the $LLL$ algorithm [4]. We express $m$ in the basis $\alpha$: $m = m_0\alpha_0 + m_1\alpha_1 + m_2\alpha_2$ ($m_i \in \mathbf{Q}$) and finally take $t = t_0\alpha_0 + t_1\alpha_1 + t_2\alpha_2$ where $t_i$ is the closest integer to $t_i$. This algorithm gives the point $t$ nearest to $m$ within a factor $K$ which is analysed in [1]. If $n$ is sufficiently large compared to $1/\epsilon$, this factor will be of order $n^{\epsilon/3}$.

## II.3. The uniqueness problem

Here come up some geometrical facts about lattices $M$ which have their shortest vector $\lambda_1(M)$ not too small, namely

$$\|\lambda_1(M)\|_\infty \geq \mu_0$$

If we define $\mu_1 = \mu_0/K$, we then have the following facts for any euclidean ball $B(m, r)$:

i) If $r < \mu_0/2$, then $B(m, r)$ contains at most one point of $M$.

ii) Moreover, if $r < \mu_1$, the ClosePoint algorithm outputs 'empty' if no point of $M$ is in $B(m, r)$, and $t$ if $t$ is the only point of $M$ in $B(m, r)$.

So, in a such a lattice, we can get our uniqueness result.

## II.4. The analysis of the lattices $M(x_0)$

Are there many lattices $M(x_0)$ which have their shortest vector not too long ? We have the following answer ([3], [9])

*For any $n, \epsilon > 0$, for any triple $k = (k_0, k_1, k_2)$ of product 1, there exists an exceptional subset $T(\epsilon)$ of $Z(n)$ such that the following is true:*

*i) Card $T(\epsilon) \leq n^{1-\epsilon}$*

*ii) For any $x_0$, not in $T(\epsilon)$, the shortest vector $\lambda_1(M(x_0))$ of the lattice $M(x_0)$ satisfies*

$$\|\lambda_1(M(x_0))\|_\infty \geq n^{(1-2\epsilon)/3} \tag{3}$$

We deduce that we can apply the facts described in 2.3 to most of lattices $M(x_0)$ provided we choose

$$\mu_0 = n^{(1-2\epsilon)/3} \quad \text{and also} \quad \mu_1 = n^{1/3-\epsilon}.$$

We know also that we can decide whether we are in $T(\epsilon)$.

## II.5. The end of the proof

If $(x, y)$ is a compatible pair in $J(a, x_0) \times I(b, y_0)$, we want to find it. This pair $(x, y)$ gives a point $w = (u_1^2, u_1 u_2, y_0 + v - u_2^2)$ of $L(x_0)$, then a point $t = (k_0 u_1^2, k_1 u_1 u_2, k_2(y_0 + v - u_2^2))$ of $M(x_0)$.

We now choose the triple $k$ so that all the approximations be bounded by $\mu_1$ : if we let $k_0 = k_1 = \lceil n^c \rceil$ , we require

$$2a + b = 1 - 3\epsilon \quad \text{and} \quad c = (b - a)/3 \tag{4}$$

Let $m = (0, 0, k_2 y_0)$; then $t$ is in the ball $B(m, \mu_1)$. The ClosePoint algorithm finds a point $t'$ in $B(m, \mu_1)$. As this ball contains only *one* point belonging to $M(x_0)$, we must then have $t = t'$. From $t'$, it is then easy to get $u_1$ by ordinary square root extraction, and then $u_2$ and $v$; we then verify if $u_1, u_2, v$ satisfy (1). This ends the proof of Theorem 1.

We remark that the optimal choice for the pair $(a, b)$ is

$$a = b = 1/3 - \epsilon.$$

## II.6. Back to the breaking of Okamoto's cryptosystem

Okamoto's second cryptosystem hypotheses are a particular case of ours. He takes $a = 2/9, v = 0$; we remark that our results indeed allow to decrypt the message $y$, because most of the $x_0$'s used –here, the quotients of two easy numbers– are outside the exceptional set. Furthermore, our algorithm works even if

i) the 1/3 of the least significant bits of $y$ are lost

ii) the pair $(n, x_0)$ has no particular form.

# III. PROOFS OF THEOREM 1BIS AND THEOREM 2

Given $n, x_0, y_0, a, b$, we must find $u, v$, that satisfy

$$|u| \leq n^a, \ |v| \leq n^b \tag{5}$$

and that are solutions of the equation

$$(x_0 + u)^2 \equiv y_0 + v \ \ [n]$$

As before, replacing $u$ by $w_0$ and $v - u^2$ by $w_1$, we then have the lattice $L(x_0)$ which has for matrix:

$$\begin{pmatrix} 1 & 0 \\ 2x_0 & n \end{pmatrix}$$

with determinant $n$. We also use a second lattice $M(x_0)$, with a suitable choice of $(k_0, k_1)$ and the point $m$ is now $(0, k_1(y_0 - x_0^2))$.

### III.1. Outline of the proof of Theorem 1bis; precisions about Shamir's attack

The proof of Theorem 1bis is similar to the proof of Theorem 1: The condition (3) of lattice regularity is just replaced by

$$\|\lambda_1(M(x_0))\|_\infty \geq n^{(1-2\epsilon)/2} \qquad \text{(3bis)}$$

This result allows to make precise some points of Shamir's first attack: The underlying framework of this attack is the one of Theorem 1bis.

Why is it so often successful? We remark that the exceptional set $T(\epsilon)$ associated to the value of $\epsilon$ defined by the equality

$$p = n^{(1-\epsilon)/3}$$

does not contain any easy point $x_0$ provided that $n^\epsilon > 2$. Shamir's attack almost always succeeds !

This attack also works even if the 2/3 least significant bits of the message are lost or erroneous

### III.2. Proof of Theorem 2; an improvement of Brickell's result

There are two facts for this proof:

1) Once we get $w = (w_0, w_1)$ of $L(x_0)$ close to the point $m$, it is very easy to get $u$ and $v$ satisfying (5); we have

$$u = w_0, \text{ and } v = w_1 + u^2,$$

there are no compatibility conditions as in Theorem 1.

2) We have one more property of lattices $M(x_0)$ satisfying (3bis), which has to do with existence and not with uniqueness:

If $\mu_2 = n^{1/2+\epsilon}$, the ball $B(m, \mu_2)$ contains *at least* one point of the lattice.

Taking $k_0 = \lceil n^c \rceil$ and $k_1 = 1/k_0$, one then must have:

$$a + c = b - c = \frac{1}{2} + \epsilon,$$

so we then take $c = (b - a)/2$. The proof ends then as in Theorem 1.

Theorem 2 gives an improvement of Brickell's breaking of the signature scheme: *If one looks for an $x$ such that $x^2$ is in $I(b, y_0)$, one finds $x$ in almost any prescribed $I(a, x_0)$ as soon as $a > 1/3$.*

### III.3. Extensions to higher degrees

Most of our uniqueness results can be generalized : as is shown in [9], we can recover, in polynomial probabilistic time, roots of polynomial equations of higher degree provided that we are given a sufficiently good approximation of these roots.

## IV. BIBLIOGRAPHIC REFERENCES

[1] L. Babai: On Lovasz's lattice reduction and the nearest lattice point problem, *Combinatorica* 6 (1986), pp 1-14.

[2] E. Brickell, J. Delaurentis: An attack on a signature scheme proposed by Okamoto and Shiraishi, *Proc. of Crypto'85*, pp 10-14.

[3] A. Frieze, J. Hastad, R. Kannan, J.C. Lagarias, A. Shamir: Reconstructing truncated variables satisfying linear congruences, to appear in *SIAM Journal of Computing.*

[4] A.K. Lenstra, H.W. Lenstra, L. Lovasz : Factoring polynomials with integer coefficients, *Mathematische Annalen*, 261, (1982) pp 513-534.

[5] T. Okamoto, A. Shiraishi: A fast signature scheme based on quadratic inequalities, *Proc. of the 1985 Symposium on Security and Privacy*, April 1985, Oakland, CA.

[6] T. Okamoto: Fast public-key cryptosystem using congruent polynomial equations, *Electronics Letters*, 1986, 22, pp 581-582.

[7] T. Okamoto: Modification of a public-key cryptosystem, *Electronics Letters*, 1987, 23, pp 814-815.

[8] A. Shamir: Private communications to Okamoto, quoted in [7], August and October 1986.

[9] B. Vallée, M. Girault, P. Toffin: How to guess $\ell$-th roots modulo $n$ by reducing lattices bases, preprint of Université de Caen, to appear in *Proceedings of First International Joint Conference of ISSAC-88 and AAECC-6* (July 88).