Determining the Entries of a Boneh and Durfee Lattice Basis

Atipatsa Chiwanda Kaminga

Abstract

Dan Boneh and Glenn Durfee [1] showed that if the private exponent $d$ used in the RSA public-key cryptosystem is less than $N^{0.292}$, where $N$ is the product of two $n$-bit primes, then the system is insecure. In their approach, they build a lattice basis matrix with short vectors whose entries are coefficients of defined polynomials ($x$-shifts and $y$-shifts). We give a formula that can easily determine some entries of the $y$-shift vectors after Gaussian elimination, and we explain how to determine each entry of a "Boneh and Durfee lattice basis."

1. Introduction

An RSA public key cryptosystem consists of an integer $N$ (which is the product of two $n$-bit primes, $p$ and $q$) and two integers $e$ and $d$ satisfying $e \cdot d \equiv 1 \mod \frac{\phi(N)}{2}$, where $\phi(N)$ is the Euler totient function [2]. The integers $e$ and $d$ are called encryption and decryption exponents respectively.

It has been shown by Boneh and Durfee that given the pair, $\{e, N\}$, one can efficiently recover $d$ provided $d < N^{0.292}$. Our main interest in their work is in the lattice basis matrix which they formed in order to solve a problem called the small inverse problem. They want the basis matrix to contain vectors of as small norm as possible. In order to achieve this, they define

---

1 Adjunct Lecturer, Mathematics Department, Mzuzu University, Malawi. Email: atipatsacwichanda@yahoo.co.uk
polynomials (the $x$-shifts and the $y$-shifts) whose coefficient vectors constitute the rows of the basis matrix. Later they perform Gaussian elimination to set some entries in a row to zero. After Gaussian elimination, we concentrate on a submatrix whose rows are the $y$-shift rows in which the first $\frac{(m+1)(m+2)}{2}$ entries have been excluded. This submatrix again spans a lattice. The rows of this matrix form a basis which we call a "Boneh and Durfee lattice basis." We analyse it and show how to determine entries in each of its rows.

2. Preliminaries

2.1 A Lattice

Let $u_1, ..., u_w \in \mathbb{Z}^n$ be linearly independent vectors with $w \leq n$. A lattice $L$ is the set of all integer linear combinations of $u_1, ..., u_w$. The lattice is full rank if $w = n$ [1].

2.2 The Small Inverse Problem

Let $A = \frac{N+1}{2}$ and $f(x, y) = x(A+y)-1$. Find $(x_0, y_0)$ satisfying $f(x_0, y_0) \equiv 0 \pmod{e}$ where $|x_0| < e^\delta$ and $|y_0| < e^{1/2}$ for some $\delta$ to be determined. For simplicity, let $\lceil e^\delta \rceil = X$ and $\lceil e^{1/2} \rceil = Y$.

2.3 $x$-shift and $y$-shift Polynomials

Given a positive integer $m$ and integers $\phi = 0, ..., m$, $i = 0, ..., m - \phi$ and $\nu = 0, ..., t$ (for some $t$), we define the polynomials $g_{i,\phi}(x, y) = x^i f^\phi(x, y)e^{m-\phi}$ and $h_{\nu,\phi}(x, y) = y^\nu f^\phi(x, y)e^{m-\phi}$.

The polynomials $g_{i,\phi}(x, y)$ are referred to as the $x$-shifts while the polynomials $h_{\nu,\phi}(x, y)$ are referred to as the $y$-shifts.

Using the coefficient vectors of the polynomials $g_{i,\phi}(xX, yY)$ and $h_{\nu,\phi}(xX, yY)$, Boneh and Durfee form a matrix $M$ whose rows span a lattice $L$. Figure 1 shows the matrix $M$ for $m = 3$ and $t = 1$. 
Figure 1: The matrix whose rows are coefficient vectors of the polynomials, \( g_i,\phi(xX, yY) \) and \( h_\nu,\phi(xX, yY) \) for \( \phi = 0, \ldots, 3, i = 0, \ldots, 3 - \phi, \) and \( \nu = 0, 1. \) The symbol "," denotes a non-zero entry [1].

As you can see in Figure 1, the last four rows of the matrix are the coefficient vectors of the \( y \)-shifts while the rest of the rows are the coefficient vectors of the \( x \)-shifts. We call the rows corresponding to \( x \)-shifts \( M_x \) and the rows corresponding to \( y \)-shifts \( M_y. \)

2.4 A lattice basis Matrix \( M \)

In general, for any given \( m \) and \( t, \) \( M \) takes the form shown in Figure 2.
Figure 3: A matrix \( M \) after Gaussian elimination.

<table>
<thead>
<tr>
<th>( x )-shifts</th>
<th>( y )-shifts</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Lambda )</td>
<td>( 0 )</td>
</tr>
<tr>
<td>( M_y' )</td>
<td>( M_y )</td>
</tr>
</tbody>
</table>

In Figure 3, \( \Lambda \) is a diagonal matrix consisting of the diagonal entries from \( M_x \).

Our main interest is in the entries of the rows of \( M_y' \). Since these rows are linearly independent, they span a lattice. Thus they form a basis and it is the basis which we call a Boneh and Durfee lattice basis. We will give a formula for calculating entries in each row of \( M_y' \).

3. Determining an Entry in each row of \( M_y' \)

Recall that each row of \( M_y \) is the coefficient vector for \( h_{\nu,\phi}(x,x') \) where \( h_{\nu,\phi}(x,y) = y^\nu f^\phi e^{m-\phi} \). Since the entries in \( M_y' \) are the same as the corresponding entries in \( M_y \), we simply need to consider the coefficients of the monomials not appearing in \( x \)-shifts for \( h_{\nu,\phi}(x,x') \).

For simplicity, we do this by first expanding \( h_{\nu,\phi}(x,y) \), using the Binomial Theorem twice as \( f = Ax + xy - 1 \).

**Lemma 0.1** Let \( \nu, \phi, l \in \mathbb{Z} \) with \( 1 \leq \nu \leq t, 0 \leq \phi \leq m, \) and \( 1 \leq l \leq \nu \). The coefficient of \( x^{\nu+\nu-l}y^\rho \) in \( f^\phi \) is \( A^{\nu-l}(\phi-\nu+l)(\phi-\nu+l+\rho)(-1)^{\phi-\nu+l+\rho} \) for \( 0 \leq \rho \leq \phi - \nu + l \).

A detailed proof of this Lemma is given next page.
Proof of Lemma 0.1

\[ f^\phi = (xy + (Ax - 1))^\phi \]
\[ = \sum_{\gamma=0}^{\phi} \binom{\phi}{\gamma} (xy)^{\phi-\gamma}(Ax - 1)^\gamma \]
\[ = \sum_{\gamma=0}^{\phi} \binom{\phi}{\gamma} (xy)^{\phi-\gamma} \sum_{k=0}^{\gamma} \binom{\gamma}{k} (Ax)^{\gamma-k}(-1)^k \]
\[ = \sum_{\gamma=0}^{\phi} \sum_{k=0}^{\gamma} \binom{\phi}{\gamma} \binom{\gamma}{k} (xy)^{\phi-\gamma}(Ax)^{\gamma-k}(-1)^k \]

Thus, the coefficient of \( x^{\phi-k} y^{\phi-\gamma} \) is \( A^{\gamma-k} \binom{\phi}{\gamma} \binom{\gamma}{k} (-1)^k \).

Let \( k = \gamma - \nu + l \) and \( \rho = \phi - \gamma \).

Then, \( A^{\gamma-k} \binom{\phi}{\gamma} \binom{\gamma}{k} (-1)^k = A^{\nu-l} \binom{\phi}{\gamma} \binom{\gamma}{\nu+l} (-1)^{\gamma-\nu+l} \).

We have \((-1)^{\gamma-\nu+l} = (-1)^{\phi-\nu+l+\rho}\).

Since \((-1)^{-\rho} = (-1)^{\rho}\), it follows that \((-1)^{\gamma-\nu+l} = (-1)^{\phi-\nu+l+\rho}\).

To finish the proof, we must show that \( \binom{\phi}{\gamma} \binom{\gamma}{\nu+l} = \binom{\phi}{\nu+l} \binom{\phi-\nu+l}{\phi-\gamma} \).

\[ \binom{\phi}{\gamma} \binom{\gamma}{\nu+l} = \frac{\phi!}{\gamma!(\phi-\gamma)!} \times \frac{\gamma!}{(\nu+l)!(\gamma-\nu-l)!} \]
\[ = \frac{\phi!}{(\phi-\gamma)!(\gamma-\nu-l)!(\nu-l)!} \]

and,

\[ \binom{\phi}{\nu+l} \binom{\phi-\nu+l}{\phi-\gamma} = \frac{\phi!}{(\phi-\nu+l)!(\nu-l)!} \times \frac{(\phi-\nu+l)!}{(\phi-\gamma)!(\gamma-\nu+l)!} \]
\[ = \frac{\phi!}{(\phi-\gamma)!(\gamma-\nu+l)!(\nu-l)!} \]

Therefore, \( \binom{\phi}{\gamma} \binom{\gamma}{\nu+l} = \binom{\phi}{\nu+l} \binom{\phi-\nu+l}{\phi-\gamma} \). \( \square \)

**Theorem 0.1** Let \( m \geq 1 \), \( 1 \leq \nu \leq t \), and \( 1 \leq l \leq \nu \) be integers such that \( 0 \leq \phi \leq m \). The coefficient of \( x^{\phi+\nu-l} y^{\phi+\nu} \) in \( y^\nu f^\phi e^{m-\phi} \) is \( A^{\nu-l} e^{m-\phi} \binom{\phi}{\phi-\nu+l} \binom{\phi-\nu+l}{\phi-\rho} (-1)^{\phi-\nu+l+\rho} \) for \( 0 \leq \rho \leq \phi - \nu + l \). Note that if \( \rho < 0 \) or \( \rho > \phi - \nu + l \) then this coefficient is 0.

Proof follows immediately from Lemma 0.1.
3.1. Remarks and Conclusion

In the matrix $M_y$, we deduce using Theorem 0.1 that an entry in each row is the coefficient of $x^{\rho+\nu-l}y^{\rho+\nu}$ and is given by the formula,

$$A^{\nu-l}e^{m-\phi}\left(\frac{\phi}{\phi+1}\right)(\frac{\phi}{\rho})X^{\rho+\nu-1}Y^{\rho+\nu}(-1)^{\phi-\nu+l+p},$$

for all $0 \leq \rho \leq \phi - \nu + l$ and $1 \leq l \leq \nu$. The entry is zero if $\rho < 0$ or $\rho > \phi - \nu + l$.

Therefore, given $\phi$ and $\nu$ we can compute all the entries in a row $y^{\nu}f^{\phi}e^{m-\phi}$ of $M'_y$ without first expanding the polynomial $h_{\nu,\phi}(x, y)$.

Acknowledgments

The author is grateful to Professor Edward F. Schaefer (of Santa Clara University, USA) for his helpful comments that improved the clarity of this paper.

References
