Public–Key Encryption using Decoder Algorithm

V V S S S Balaram, K N Murty, B R Sastry

Aurora's Technological and Research Institute
Parvathapur, Uppal, Hyderabad, India

Summary
A method for finding the closest point for lattices with a regular spherical structure and a modified ML decoder for the closest vector problem (CVP) are presented. Based on the algorithm one can construct a public key encryption algorithm. A CVP algorithm using convex hull to avoid the complexity of finding radii for the existing ML decoders is also presented.

***Key Words*:**
Public-Key Encryption, Closest Vector Problem (CVP), ML Decoder.

1. Introduction

With the ever increasing confidential data being sent on the fast spreading computer networks the security aspect has become the focal point. One of the methods that has been used for various applications is the public-key encryption technique, which has been used with fair success. However, sound public-key cryptosystems are yet to be developed and a lot of work is focused on to this aspect of secure data transmission. Moreover, the source of security of these proposals may rely on the computational intractability of problem in infinite integer rings, specifically integer factorization and discrete logarithm computation.

The proposed algorithm relies on the computational difficulty of lattice reduction problem, in particular, the problem of finding closest vectors in a lattice to a given point (CVP). This method is asymptotically more efficient than the RSA and ElGamal encryption scheme, in which the computation times for encryption and decryption are quadratic in nature regarding security parameter. The new system has public key of size $O(k^2)$ and computation time also of $O(k^2)$. We define a trapdoor function for the public key encryption algorithm. It is known that given any basis for a lattice, it is easy to generate a vector which is close to a lattice point. However, it is very hard to find the "close-to-lattice" vector to the original lattice point. It is clear that different basis vectors of the same lattice seem to yield a difference in the ability to find close lattice points to arbitrary vectors in Z^n. Let us consider two different basis vectors of the same lattice – one that allows computing the function but not inverting and the other that allows computing inverse function by permitting good approximation to the closet lattice vector problem (CVP).

Manuscript received January 5, 2008
Manuscript revised January 20, 2008

We call this basis as reduced basis. Of the selected two basis vectors of same lattice, one has small dual orthogonality defect and other lattice has a large dual orthogonality defect. Given an arbitrary point $x \in Z^m$ and a generated matrix for a lattice Λ, the algorithm computes the point that is closest to x. In lattice theory, a generator matrix G is any matrix with real entries whose rows are linearly independent over Z. Let n and m denote the number of rows and columns of G respectively where $n \leq m$, the lattice generated by G is

$\Lambda(G) = \{uG : u \in Z^n\}$.

The rows of G are called basis vectors for Λ, and the number n of basis vectors is based on the dimension Λ.

The closest point problem is the problem of finding, for a given lattice Λ and a given input point $\in R^m$, a vector $\hat{c}$ such that

$$\| x - \hat{c} \| \leq \| x - c \| \text{ for all } c \in \Lambda.$$

Where $\| . \|$ denote the Euclidean norm.

An efficient closest point search algorithm based on the Eachner [2,7] - a variation of the Pohest method is implemented for lattice without regular structures.

Maximum – likelihood (ML) decoding algorithm for searching closest lattice point was proposed by [1]. Such decoding algorithms are collectively referred to as spherical decoders. These algorithms can be used in communication problems to decode the information.

This paper presents an efficient algorithm for public key encryption using modified ML decoding algorithms for finding CVP. In section II, the problem is defined and in section III an algorithm to find initial radius is proposed and a modified ML decoder algorithm for finding closest lattice point is presented. In section IV another algorithm to find closest vector using convex hull is proposed. In section V conclusion and remarks are given.

I. Problem Formulation and Preliminaries

The public-key Encryption scheme [3] is based on a trapdoor function and is defined in the usual way. That is, to encrypt a message we embed it inside the argument of the function, process it to generate the cipher text. To decrypt, one uses trapdoor information to invert the function and extract the message from the argument.

One way to generate a trapdoor function is to take a lattice vector and adding a small error vector. Received data may be visualized as a linear combination of the base vector and error vector of data. Consider the following linear model

$y = Bx + e$ (1)

Where $x \in R^n$, $y \in R^n$ and e denote the plaintext and ciphertext and error term respectively and $B \in R^{m \times m}$ is a generate matrix.

$\Lambda(B) = \{\lambda : \lambda = Bz, z \in Z^m\}$, where B is known at the receiver.

The error vector $e(e_1 \ldots\ldots e_p)$ is independent and identically distributed and is to be minimized.

The problem may be reduced to minimizing the squared Euclidean distance to a target vector $\hat{x}$ over an M dimensional discrete search $C \in Z^m$

Our problem is to find $\hat{x}$ such that

$\hat{x} = \text{argmin} \| y\text{-}Bx \|^2$ (2)

Where $\| \ \|$ is a Euclidean distance which is to be minimized.

The set $\Lambda = \{Bx : x \in z^m\}$ is a M dimensional lattice in Z^n. The search methodology in (2) for the closest lattice point to a given point y has been widely discussed in lattice theory. All problems related to general lattices that do not exhibit any particular structure were shown to be NP – hard. Pohst [2] proposed an efficient strategy for finding all the lattice points with a sphere of a certain radius, that can give polynomial solutions.

Pohest enumeration is briefly outlined below. Let C_0 be the squared radius of an n – dimensional sphere S(y, √Co) centered at y. We can find all points of $\Lambda \in$ S (y, √Co) by applying QR decomposition on B which is given by

$$B = [Q, Q^1] \begin{bmatrix} R \\ O \end{bmatrix} \quad (3)$$

Where R is an m×m upper triangular matrix with positive diagonal elements, O is null matrix of size (n-m) ×m and Q and Q^1 are unitary matrices of size n×m and n×(n-m) respectively. The condition $Bx \in$ S (y, √Co) can be written as

$$| y - Bx |^2 \le C_0$$

$$| [Q, Q^1]^T y - \begin{bmatrix} R \\ O \end{bmatrix} x |^2 \le C_0$$

$$| Q^T y - R_x |^2 \le C_0 - |(Q^1)^T y |^2$$

$$| y^1 - R_x |^2 \le C_0^1$$

Where $y^1 = Q^T y$ and $C_0^1 = C_0 - | (Q^1)^T y |^2$

Because R is an upper triangular, the last inequality implies the set of conditions

$$\sum_{j=i}^{m} | y_j^{/} - \sum_{l=j}^{m} r_{j,l} x_l |^2 \le C_0^1, \ i = 1 \ldots m \quad (4)$$

By considering the above conditions in the order from m to 1, we obtain the set of admissible values of each vector x_i for given values of symbols $x_{i+1}, \ldots, x_m$ .More clearly, let $x_l^m = (x_l, x_{l+1}, \ldots, x_m)^T$ denote the last m-l+1 components of the vector x. For a fixed x_{i+1}^m the component x_i can take values in the range of integers $I_i (x_{i+1}^m)$`

$[A_i (x_{i+1}^m), B_i (x_{i+1}^m)]$ where

$$A_i (x_{i+1}^m) = [\frac{1}{r_{i,i}} (y_i^1 - \sum_{j=i+1}^{m} r_{i,j} x_j - \sqrt{C_0^1 - \sum_{j=i+1}^{m} | y_j^1 - \sum_{l=j}^{m} r_{j,l} x_l |^2})]$$

$$B_i (x_{i+1}^m) = [\frac{1}{r_{i,i}} (y_i^1 - \sum_{j=i+1}^{m} r_{i,j} x_j + \sqrt{C_0^1 - \sum_{j=i+1}^{m} | y_j^1 - \sum_{l=j}^{m} r_{j,l} x_l |^2})] \quad (5)$$

If $\sum_{j=i+1}^{m} | y_j^l - \sum_{l=j}^{m} r_j 1, l x_l |^2 > C_0^1$ or

if $A_i (x_{i+1}^{1m}) > B_i (x_{i+1}^m)$, then $I_i ((x_{i+1}^m) = \phi$ (empty set)

So no value of x_i satisfies the inequality (4) and the points corresponding to this choice of x_{i+1}^m do not belong to the sphere S(y, √C_0).

Pohest enumeration is based on the natural spanning of the intervals $I_i (x_{i+1}^m)$ at each level i, i.e., x_i takes on values in the order $A_i (x_{i+1}^m)$, $A_i (x_{i+1}^m) + 1$,.., $B_i (x_{i+1}^m)$. But in Schnorr – Euchner enumeration, the intervals are taken in a zig-zag order, starting from the mid point and the interval. The interval boundaries are modified as

$A_i (x_{i+1}^m) =$

$$\max \left\{ 0, \left| \frac{1}{r_{i,i}} \left(y_i^{/} - \sum_{j=i+1}^{m} r_{i,j} x_j - \sqrt{C_0^{/} - \sum_{j=i+1}^{m} \left| y_j^{/} - \sum_{l=j}^{m} r_{j,l} x_l |^2 \right)] \right\} \right.$$

$B_i (x_{i+1}^m) =$

$$\min \left\{ Q - 1, \left| \frac{1}{r_{i,i}} \left(y_i^{/} - \sum_{j=i+1}^{m} r_{i,j} x_j + \sqrt{C_0^{/} - \sum_{j=i+1}^{m} \left| y_j^{/} - \sum_{l=j}^{m} r_{j,l} x_l |^2 \right)] \right\} \right. \quad (6)$$

In the above procedure, finding a vector $x \in Z^m$, which belongs to $B_x \in$ S (y, √C_0) depends on the initial value of C_0. An initial value for C_0 as input value of the decoder algorithm is assumed by trail and error method and modifying gradually by steps until one finds the lattice point. In general, the proper initial value of C_0 is critical in order to reduce the complexity of the algorithm. If C_0 is

small the resultant search may be empty and may not yield the result whereas a too large C_0 may result in too many points to be enumerated for finding the solution. The limitation of Phost algorithm may be overcome by considering the set of points that are close to the centre y and calculating the initial radius [6] using the proposed algorithm which will greatly reduce the complexity of the algorithm for finding the closest vector. It is also optimal as we consider dot product in numerical computations to find out the farthest point from y.

2. CVP Algorithm Using Modified ML Decoder

Given a finite set of points P in Z^d, the diameter D of P is defined as the maximum distance between two points of P. We denote by n the number of points of P, by h the number of vertices of the convex hull of P and δ (.,.) the Euclidean distance. The length of a segment of a pair of points pq is the Euclidean distance δ (p,q) between p and q. For p ∈ P, FP(p) denotes the subset of the points of P that are at maximal distance from p.

The segment joining two points p and q is called double normal if p ∈ FP(q) and q∈FP(p). If pq is a maximal segment, pq is a double normal. The converse is not necessarily true.

Using the following normal algorithm we find double normal (DN) of a point P until a maximal DN is found. We compare the distance between y and all the other points in P and find a farthest neighbour of p∈P. If yp is not maximum, p is then removed from P. Given the centre y and consider the set of random points, the double normal is calculated using the following algorithm.

Algorithm

1. Procedure DN (y, P)
2. $D_0^2 = 0$ i= 0
3. repeat
4. increment i
5. $D_i^2 = D_{i-1}^2$
6. find q∈FP(y), that is one of the farthest neighbors of y
7. if δ^2(y,q) > D_i^2 then
8. $D_i^2 = \delta^2$(y,q) and DN = yq
9. consider next point q∈FP(y)
10. Repeat steps 7 to 10 until all points are over.
11. return DN

The calculated double normal gives us the diameter from centre y, based on which C_0 is calculated. This diameter is given as input to the following algorithm to find closest vector.

1) Apply the pohest enumeration with the internal boundaries modified as

$A_i\ (x_{i+1}^m) =$

$$\max\left\{0, \left|\frac{1}{r_{i,i}}\left(y_i' - \sum_{j=i+1}^{m} r_{i,j}x_j - \sqrt{C_0' - \sum_{j=i+1}^{m}\left|y_j' - \sum_{l=j}^{m} r_{j,l}x_l\right|^2}\right)\right|\right\}$$

$B_i(\ x_{i+1}^m) =$

$$\min\left\{Q-1, \left|\frac{1}{r_{i,i}}\left(y_i' - \sum_{j=i+1}^{m} r_{i,j}x_j + \sqrt{C_0' - \sum_{j=i+1}^{m}\left|y_j' - \sum_{l=j}^{m} r_{j,l}x_l\right|^2}\right)\right|\right\}$$

and obtain the list of all vector x∈z^m such that Bx ∈ S(y, $\sqrt{C_0}$)

2) If the list is nonempty, output the point having minimum distance

Algorithm (input C_0^1, y^1, R, output $\hat{x}$)

1) set i=m, $T_m = 0$, $\xi_m = 0$ $d_c = C_0^1$ // initialize the variables

2) if $d_c < T_i$ go to step (4) else (bounds on x)

calculate $A_i\ (x_{i+1}^m)$ and $B_i(\ (x_{i+1}^m)$ using the above equations

set $x_i = A_i\ (x_{i+1}^m)$ -1

3) $x_i = x_i + 1$

If $x_i \le B_i\ (x_{i+1}^m)$ go to step 5, else go to step 4.

4) If i=m terminate,

else set i=i+1 and go to step (3)

5) decrement i: move one level up. If i>1, then

{let $\xi_{i-1} = \sum_{j=i}^{m} r_{i-1,j}x_j, T_{i-1} = T_i + |\ y_i' - \xi_i - r_{i,i}x_i|^2$, let i=i-1 go to step (2)}

6) A valid point is found by calculating

$\hat{d} = T_1 + |\ y_1' - \xi_1 - r_{1,1}x_1|^2$

If $\hat{d} < d_c$ then $d_c = \hat{d}$, save $\hat{x} = x$, and update the upper boundaries

$B_l\ (x_{l+1}^m) = \min\{Q-1, [\ y_l' - \xi_1 + \sqrt{d_c - T_l}]\}$ for all l = 1,…,m}, go to step (3)

3. Closet Vector Algorithm Using Convex Hull

In the above algorithm a method of finding CVP for the spherical region of points that may take a lot of iterations is

discussed. A more efficient algorithm is proposed by considering convex hull region to find CVP. After constructing convex hull [4,5], Euclidean distances from the centre (y) to all these points which are inside the constructed region (convex hull) are found and from these, the minimum distance is identified that gives the closest vector. For finding the initial points, we consider B, the generate matrix given in equation (2) and apply QR decomposition on B, to find all points $\Lambda \in S$ (y,√Co). The QR decomposition on B is given by

$$B = [Q\ Q^1] \begin{bmatrix} R \\ O \end{bmatrix}$$

Where R is an m×m upper triangular matrix with positive diagonal elements, O is an
(n-m) × m zero matrix Q and Q^1 are unitary matrix with size n×m and n× (n-m) respectively. Consider matrix R as an input to the following algorithm.

The convex hull of a set of points is defined as the smallest convex set that contains the points and is mostly used in computational geometry. We represent a convex hull with a set of facets and a set of adjacency list giving the neighbors and vertices for each facets. The boundary elements of a facet are called ridges. Each ridge signifies the adjacency of two facets and in R^3 position, facets form triangles and ridges form edges. We represent an n-dimensional convex hull by its vertices and (d-1) dimensional faces (facets). The out line of the convex hull algorithm is given below :

Algorithm Convex Hull (y,R).

1) Consider the points in the matrix R
2) For each facet F
   For each unsigned point p if p is above F
   p = pU{O} where O is a outside set.
3) For each facet F with a non-empty outside set
   select the farthest point p from the set {O}
   initialize the visible set V to F.
4) For all unvisited neighbors N of facets in V
   if p is above N
   add N to V
   The set of horizon ridges H is the boundary of V
5) For each ridge R_g in H
   Create a new facet from R_g and p
   link the new facet to it neighbors
6) For each new facet F^1
For each unassigned point q in an outside set of a facet in V
7) If q is above F^1 assign q to $F^/$ out side set
8) Delete the facets in V

After construction of the convex hull, each and every internal point is considered to find the Euclidean distance from centre y using the following algorithm.
Algorithm Distance (y, point of convex hull)

1) dim = m
2) while (dim>0)
3) begin
   sum = sum + pow (y[i]_x[i++]),z);
   end
   decrement Dim;

From the above one can find the minimum distance which gives the closest lattice point.

4. Conclusions

Multi-point communication have recently become the focus of new developments in the area of network of group communications such as video-conferencing and network layer multicast protocol. We propose a new framework for multicast security based on the lattice reduction problems. For constructing such type of algorithm we consider the following linear model.

$$y_r = Bx_r + e_r$$

Where r represents the number of receivers. Consider the minimization problem

$$\hat{x}_r = \text{argmin} \parallel y_r - Bx_r \parallel^2$$

Where $\| \ \|$ denote the Euclidean norm. Using the above equations, a new lattice based algorithm that suits better for group communication is proposed.

REFERENCES

[1] M O Damen Hesham El Gamel and Giuseppe Caire, "is on maximum-likelihood detection and search for the closest lattice point", IEEE trans inform theory, vol. 49, pp.2389-2402, Oct.2003.
[2] E Agrell Eriksson, Vardy, and Zeger, "Closest point search in lattices", IEEE trans inform theory, Vol.48, pp.2201-2214, Aug.2002.
[3] M Ajtai and C Dwark, "A Public-key cryptosystem with worst-case/average-case Equivalence", In 29th ACM symposium on theory of computing, pp 284-293, 1997.
[4] C Bradford barber, David P Pobkin and H Hurdanpace "The quick null algorithm for convex hulls", submitted to the ACM transactions on mathematical software, Jan 1995.
[5] N M Amato, M T Godrich, and E A Ramos. "Parallel algorithms for higher dimensional convex hulls", In Proc. 35th Annu. IEEE Sympos. Found comput.Sci., pp 683-694, 1994.
[6] S Bespamyatnikh, "An efficient algorithms for three-dimensional diameter problem", In Proc. 9th Annu. ACM-SIAM Symp. Discrete Algorithms, pp 137-146, 1998.
[7] B R Sastry, K N Murty, V V S S S Balaram, " General First order matrix Difference System – existence and uniqueness via New Lattice based Cryptographic constriction" , Electronic Modeling, V.29, No. 2 07.

V V S S S Balaram is currently with Aurora's Technological and Research Institute, working as Assistant Professor in the Department of Information Technology. He has 15 years of teaching experience. He did his M.Tech from Andhra University and Pursuing his Ph.D under the guidance of Dr. B.R. Sastry from Osmania University. His areas of interest include Network Security and Cryptography, Operating System, Distributed Operating Systems and Computer Graphics. He has a few International Publication to his credit. (corresponding author address Aurora's Technological And Research Institute, Parvathapur, Uppal, Hyderabad, India – 500039 Phone No.91-040-27568819
Email: vadrevu_kinnera@yahoo.com)

Dr. K.N. Murty is currently the Dean of Academic Affairs, RIT, Visakhapatnam. He published 117 papers in various international mathematical journals. He was awarded best Research Award for PhD in Andhra University. He is a Reviewer for mathematical research papers for AMS (American Mathematical society).

Dr. B. R. Sastry is currently working as Dean, Academics, Aurora's Technological and Research Institute. He earlier worked for 12 years in Industry that developed indigenous computer systems in India. His areas of research includes Computer Architecture, Network Security, Software Engineering, Data Mining and Natural Language Processing,. He is currently concentrating on improving academic standards and imparting quality engineering education. He is widely traveled and a connoisseur of fine arts.