Abstract

Many of the public key cryptosystems deal with two-party communication keeping confidentiality and authentication as primary goals. However there are many applications like banking that require multi-party communication. In bank, we keep valuable articles in lockers. We need two dependent keys to open the locker. In corporate sector it may be thought of as multi-party communication. RSA provided multi-party communication using shared key approach. But the overhead of RSA seem to be more because it has to choose n pairs of numbers such that the summation of these numbers is a large prime number. This needs to be done without revealing the shares of the numbers [1, 2].

This paper proposes an algorithm for shared key authentication based on Lattice approach of NTRU for communication using dependent private key. This cryptosystem does not require
these overheads.

Reference

- Rakesh Nayak, C.V.Sastry, Jayaram Pradhan, “A matrix formulation for NTRU cryptosystem,” Proceedings 16th IEEE, International Conference on Networks (ICON-2008), New Delhi, from date 12th-14th Dec’08.
- User Manual of “Mathematica 5.1”.

Index Terms

Computer Science  Security

Key words
<table>
<thead>
<tr>
<th>Polynomial</th>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matrix</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>