

## A new key exchange protocol using two layers of security

T. Isaiyarasi \*

*Department of Mathematics  
Bharathiar University  
Valliammai Engineering College  
Coimbatore  
India*

K. Sankarasubramanian

*Department of Mathematics  
Bharathiar University  
Sri Sairam Engineering College  
Coimbatore  
India*

---

### Abstract

In this paper we present a New Key Exchange Protocol with two layers of security. For this purpose, we consider Discrete Heisenberg Group as our platform group. Firstly by considering the Triple Decomposition Problem in Discrete Heisenberg group we arrive at a shared secret key: This forms the first layer of security. Then we make use of this key in forming the Key exchange Protocol using Twisted Conjugacy Search problem implemented in the Discrete Heisenberg group.

---

**Keywords:** *Key Exchange, Triple Decomposition, Twisted Conjugacy and Discrete Heisenberg Group*