Abstract

In this article, a novel public key cryptosystem is introduced by using an abelian subgroup of $\text{GL}(k;\mathbb{Z}_n)$ where $n$ and $k$ are positive integers. Instead of exponentiation, the conjugation automorphisms are mainly used to define the public and private keys. This allows the calculations to be fast and effective. The security analysis of the cryptosystem is discussed and it is shown that the cryptosystem is highly secure. Moreover, proposed scheme also generalizes the main scheme given in [1].

References


Index Terms

Computer Science

Security

Keywords

Lower Triangular Matrices, General Linear Group, Public Key Cryptosystems