We present a secret sharing scheme whose security can be reduced to the hardness of the Learning With Errors (LWE) problem. This is a strong property since the LWE problem is believed to be very hard, as hard as worst-case lattice problems hence offering security in the quantum world. The scheme has certain technical advantages: it requires only basic operations and it allows sharing several secrets at the same time.

Reference


Index Terms

Computer Science Security

Key words

secret sharing

learning with errors

lattices