Abstract

RSA is a popular public key cryptosystem. The security of the RSA relies on the difficulty of prime factoring large composite numbers. So we need to evaluate the size of composite numbers that can be prime factorized. For numbers of the form $N = pq$ (p, q is prime) used in the RSA, the largest number of bits that is currently prime factorized is 829 bits. The algorithm used for this prime factorization is the number field sieve (NFS).

The prime factorization method used in the inside NFS is briefly explained. Suppose x, y are given that satisfy $x^2 \equiv y^2 \pmod{N}$. Then the greatest common divisor $\gcd(x \pm y, N)$ may be a prime factor of N. When prime factors of N are obtained, the prime factorization can be done. To use this prime factorization method, we need to find x, y. In the NFS, we collect several expressions of a certain form (called the factor-relation) and use them to obtain x, y.

There are two types of prime factorization algorithms using lattices proposed by Schnorr that perform prime factorization in a manner similar to the NFS. The algorithm is based on the shortest vector problem (SVP) and the closest vector problem (CVP). Both algorithms are based on computational problems in the lattice. SVP is the problem of finding the shortest vector in a lattice. CVP is the problem of finding a vector in a lattice that is close to a given vector. This paper describe about an algorithm based on SVP. This algorithm constructs a lattice and then collects factor-relations from short vectors in the lattice, and it is stated that it is capable of prime factorizing large numbers. However, the effectiveness of the algorithm has not been fully analyzed at present, so we discuss the effectiveness of the algorithm.

The algorithm based on SVP constructs two values u, v from short vectors in the lattice. If $u - vN$ is small, factor-relation is reliably obtained. Specifically, when the n-th prime number is p_n, if $u - vN \leq p_n$, the factor-relation can be obtained reliably. So assuming that the shortest vector in the lattice was obtained, we obtained the order of computational complexity of the values related to $u - vN$ from the upper bound of the norm of the shortest vector. We then investigated the behavior of $|u - vN|$ when each parameter of the lattice was varied. The results show that $u - vN$ cannot be manipulated to a value smaller than p_n From this result, an algorithm based on SVP cannot reliably obtain factor-relation. So it is thought that difficult to factorize large composite numbers. Also the algorithm was implemented and tested for every 10 bits from a 20-bit composite number and successfully prime factorized a composite numbers up to 50 bits. This result also suggests that it is difficult to prime factorize composite numbers with a large number of bits.