

Application of Zeta Function to Quantum Cryptography

Dr. Xiangdong Li¹ and Dr. Michael Anshel²

1. CUNY NYC College of Technology
2. CUNY The City College

A central problem in cryptography is to establish the existence of one-way function. We introduce a new class of one-way functions based on the arithmetic theory of Zeta functions and recent research on quantum algorithms on Zeta function computation.

Quantum key distribution (QKD) has abstracted strong interests of scientists since it makes it possible to set up unconditional secure key between two remote parties by principles of quantum mechanics.

The recently exciting news is that an electronic money transaction has been carried out in at a bank in Austria using entangled photons to create an unbreakable communications code presented by Poppe *et al.*
Opt. Express **12**, 3865-3871 (2004).

This is the first time in a real world application scenario of the entangled state quantum cryptography system. The generated quantum key was immediately handed over and used by a secure communication application.

A one-way function is a function F such that for each x in the domain of F , it is easy to compute $F(x)$; but for essentially all y in the range of F , it is an intractable problem to find an x such that $y = F(x)$.

Anshel and Goldfeld have introduced a new intractable problem arising from the theory of Zeta functions, which leads to a new class of one-way functions based on the arithmetic theory of Zeta functions.

Duke Math. J., 88, No. 2, 371-390(1996)

Recently, Shor has introduced a new approach to attack these problems.

In fact, Shor has shown that on a quantum computer the integer factorization and discrete logarithm problems can be computed in polynomial time.

Can we find a quantum algorithm to compute the elliptic curve of Zeta function?

Quantum Computing

A quantum state of n quantum bits (qubits) is described by a 2^n dimensional complex valued vector, which represents a superposition over all possible n bit strings $\{0, 1\}^n$.

It is well-known that quantum Fourier transform can be implemented efficiently on a quantum computer (with circuit depth $\text{poly}(\log n)$ and $\text{poly}(\log p^r)$ respectively).

This fact is an important ingredient of the efficient quantum algorithms for factoring and the discrete logarithm problem.

Van Dam interprets the roots of Zeta as the spectrum of a quantum mechanical process. The roots of the Zeta functions all lie on a circle in the complex plane and for curves the distribution of the zeroes of the Zeta functions obeys the 'eigenvalue repulsion' that one also sees in random quantum mechanical systems.

Kedlaya exhibits a quantum algorithm for determining the Zeta function of a genus g curve over a finite field F_q , which is polynomial in g and $\log(q)$.

zrXiv:math.NT/0411623, (2004)

The candidate one-way functions $F_{\text{Kronecker}}$, F_{Elliptic} , and F_{Artin} presented provide the basis for numerous cryptographic applications.

M. Anshel and D. Goldfeld, Duke Math. J., 88, No. 2, 371-390(1996)

Pseudorandom Number Generator

A pseudorandom number generator is a deterministic polynomial time algorithm that expands short seeds into longer bit sequences such that the output of the ensemble is polynomial-time indistinguishable from a target probability distribution.

Research

Can we find a proper quantum algorithm to compute this $P_{NGElliptic}$ which can be computed very efficiently and at low computational cost?