The value of each bit in a classical computer is either 0 or 1. In a quantum computer, each so-called quantum bit (qubit) may simultaneously takes on every value between 0 and 1 with varying probabilities. This added flexibility allows many computations, including integer factorization and discrete logarithm problems, to be done very quickly. Thus a working quantum computer with sufficiently many qubits would break RSA and both the classical and the elliptic curve versions of Elgamal. (However, there is at present no polynomial-time quantum algorithm that solve the shortest or closest lattice vector problems.)

Tempting though it is, we will not use this opportunity to give a serious introduction to quantum mechanics. The aim of this section is fairly modest. We sketch the basic ideas behind one remarkable application of quantum mechanics to cryptography: Shor's polynomial-time quantum algorithm [128] for factoring integers and for finding discrete logarithms. The following presentation owes a great deal to Shor's accessible and beautifully written exposition [129], which would serve as a nice start for the interested reader familiar with the concept of a Hilbert space. For those with a less robust background in mathematics and quantum theory, see for example [64].

The fundamental unit of information in classical computers is the binary digit (bit), represented as a 0 or 1. Bits are manipulated according to the principles of Boolean logic, in which connectives such as AND and OR operate on pairs of bits in the usual way, and NOT reverses 0 and 1. Sequences of bits are manipulated by Boolean logic gates, using these Boolean rules, and a succession of gates yields an end state, or computation. A quantum computer manipulates quantum bits (qubits) via quantum logic gates, which are supposed to simulate the laws of quantum mechanics, especially properties such as superposition and entanglement, which give the field of quantum mechanics its distinctive nonclassical characteristics.

A qubit with two states is typically represented using ket notation, in which $|0\rangle$ denotes the 0-state and $|1\rangle$ the 1-state. Then the (pure) states of the system have the form

$$\alpha\,|0\rangle + \beta\,|1\rangle\,,$$

where $\alpha$ and $\beta$ are complex numbers satisfying $|\alpha|^2 + |\beta|^2 = 1$. In an $n$-component system, the $2^n$ basis elements are represented by sequences such as $|s_i\rangle = |0110\ldots0\rangle$ consisting of a list of n zeros and ones, and a state of the system is

$$\sum_{i=0}^{2^n-1} \alpha_i\,|s_i\rangle\,, \qquad where \sum |\alpha_i|^2 = 1. \tag{8.3}$$

A sum (8.3) is called a superposition of states. There are other quantum states known as "mixed" states that we do not discuss here, so we omit the word pure in the rest of this discussion. Thus a quantum state is represented by a vector of complex numbers of length $2^n$ such that sum of the squares of their moduli is equal to one. These are called complex unit vectors.

Just as for classical computers, manipulating qubits via quantum logic gates requires the notion of a change of state. A quantum change of state is the result

of applying a unitary linear transformation16 to one of the complex unit vectors representing a state. Actually, there are additional restrictions on which unitary transformations are permitted for changes of state. One of these restrictions is the requirement of locality : the unitary matrices should operate on only a fixed finite number of bits. It turns out that 2-bit transformations form the building blocks of the allowable transformations.

The quantum-mechanical interpretation of the $\alpha_i$'s is that $|\alpha_i|^2$ represents the probability that a measurement of the system yields state $|s_i\rangle$. It is the probabilistic interpretation of the complex coefficients of these vectors that encodes the physical realities observed in experiment and predicted by physical theory.

In [129], Shor describes a quantum polynomial-time algorithm to find (with high probability) the order $r$ of a number $x \mod n$. (Recall that the order of $x$ is the smallest integer $r \geq 1$ such that $x^r \equiv 1 \mod n$.) Factorization can be reduced to the problem of finding the order of an integer, because if $x$ is chosen randomly and has even order $r$, then $\gcd(x^{r/2} - 1, n)$ is likely to be a nontrivial odd factor of $n$. (See [87].) Shor also gives a polynomial-time quantum algorithm to solve the discrete logarithm problem in $\mathbb{F}_p^*$, and such algorithms also exist for the elliptic curve discrete logarithm problem [107].

Interestingly, there are still no polynomial-time (or even subexponential-time) quantum algorithms to solve the shortest or closest vector problems, so lattice based cryptosystems are currently secure even against the construction of a quantum computer.

The basic building block of Shor's algorithm is a quantum version of the Fast Fourier Transform. In order to find the order $r$ of a number a modulo $n$, we choose $q$ to be a power of 2 in the interval between $n^2$ and $2n^2$. Then for any $0 < a < q$, the state $|a\rangle$ is obtained from the binary representation of the number $a$. The Fourier transform of $|a\rangle$ is the state

$$\frac{1}{q^{1/2}} \sum_{c=0}^{q-1} |c\rangle \exp(2\pi i ac/q)$$

It turns out that this transformation can be achieved in polynomial time. Shor then applies the quantum Fourier transform to a certain superposition of states and measures the resulting system. The key computation shows that the probability of seeing state $|c\rangle$ is relatively large if there exists a rational number $\frac{d}{r} \in$ satisfying

$$\left| c - \frac{d}{r} \right| < \frac{1}{2q}.$$

(Recall that $r$ is the order of $a$.) Using the continued fraction expansion of the known rational number $\frac{c}{q}$ it is not hard to determine the fraction $\frac{d}{r}$ in lowest terms, since $q > n^2$.

There remains only the "minor" challenge of building a functioning quantum computer. Research in this field has focused on the issue of decoherence, which involves controlling the errors in quantum computation introduced by

the interaction of the computer with its environment. There is already a vast literature on quantum computing and quantum computers, reflecting to some extent the large amount of government funding that has been allocated to the subject. One place to start gathering resources about quantum computers is the website for NIST's Quantum Information Program at qubit.nist.gov.

Finally, we would be remiss if we did not mention the theory of quantum cryptography. The idea is to use quantum-mechanical principles such as the Heisenberg uncertainty principle or the entanglement of quantum states to perform a completely secure key exchange. In particular, if Eve attempts to read either Bob's or Alice's transmission, then quantum theory says that she must alter the data, so Bob and Alice will know that their communication has been compromised.