Quantum Public-Key Cryptosystems

Tatsuaki Okamoto, Keisuke Tanaka, and Shigenori Uchiyama

NTT Laboratories
1-1 Hikari-no-oka Yokosuka-shi, Kanagawa-ken 239-0847, Japan
{okamoto, keisuke, uchiyama}@isl.ntt.co.jp
Tel: +81-468-59-2511
Fax: +81-468-59-3858

Abstract. This paper presents a new paradigm of cryptography, *quantum public-key cryptosystems*. In quantum public-key cryptosystems, all parties including senders, receivers and adversaries are modeled as *quantum* (probabilistic) poly-time Turing (QPT) machines and only classical channels (i.e., no quantum channels) are employed. A *quantum trapdoor one-way function*, f, plays an essential role in our system, in which a QPT machine can compute f with high probability, any QPT machine can invert f with negligible probability, and a QPT machine with trapdoor data can invert f. This paper proposes a concrete scheme for quantum public-key cryptosystems: a quantum public-key encryption scheme or quantum trapdoor one-way function. The security of our schemes is based on the computational assumption (over QPT machines) that a class of subset-sum problems is intractable against any QPT machine. Our scheme is very efficient and practical if Shor's discrete logarithm algorithm is efficiently realized on a quantum machine.

1 Introduction

1.1 Background and Problem

The concept of public-key cryptosystems (PKCs) introduced by Diffie and Hellman [18] and various theories for proving the security of public-key cryptosystems and related protocols (e.g., [22]) have been constructed on the Turing machine (TM) model. In other words, public-key cryptosystems and related theories are founded on Church's thesis, which asserts that any reasonable model of computation can be efficiently simulated on a probabilistic Turing machine. However, a new model of computing, the quantum Turing machine (QTM), has been investigated since the 1980's. It seems reasonable to consider a computing model that makes use of the quantum mechanical properties as our world behaves quantum mechanically. Several recent results provide informal evidence that QTMs violate the feasible computation version of Church's thesis [17, 38, 37]. The most successful result in this field was Shor's (probabilistic) polynomial time algorithms for integer factorization and discrete logarithm in the QTM model [37], since no (probabilistic) polynomial time algorithm for these problems has been found in the classical Turing machine model.

Although Shor's result demonstrates the positive side of the power of QTMs, other results indicate the limitation of the power of QTMs. Bennett, Bernstein, Brassard, and Vazirani [5] show that relative to an oracle chosen uniformly at random, with probability 1, class NP cannot be solved on a QTM in time $o(2^{n/2})$. Although this result does not rule out the possibility that NP $\subseteq$ BQP, many researchers consider that it is hard to find a probabilistic polynomial time algorithm to solve an NP-complete problem even in the QTM model, or conjecture that NP $\not\subseteq$ BQP.

Shor's result, in particular, greatly impacted practical public-key cryptosystems such as RSA, (multiplicative group/elliptic curve versions of) Diffie–Hellman and ElGamal schemes, since almost all practical public-key cryptosystems are constructed on integer factoring or the discrete logarithm problem. Therefore, if a QTM is realized in the future, we will lose almost all practical public-key cryptosystems. Since public-key cryptosystems are becoming one of the infrastructures of our information network society, we should resolve this technical and social crisis before a QTM is realized.

1.2 Our Results

This paper proposes a solution to this problem. First we show a natural extension of the concept of public-key cryptosystems to the QTM model, the *quantum public-key cryptosystem (QPKC)*. The classical model, TM in PKC, is replaced by the quantum model, QTM in QPKC. That is, in QPKC, all parties in QPKC are assumed to be (probabilistic) polynomial time QTMs. All channels are classical (i.e., not quantum) in our model of QPKC. We can naturally extend the definitions of one-way functions, trapdoor one-way functions, public-key encryption, digital signatures, and the related security notions.

We then show a concrete practical scheme to realize the concept of QPKC. The proposed scheme is a quantum public-key encryption (QPKE) scheme, or quantum trapdoor one-way function. The security of our scheme is based on the computational assumption (over QPT machines) that a class of subset-sum problems (whose density is at least 1) is intractable against QTM adversaries[1]. In this scheme, the underlying quantum (not classical) mechanism is only Shor's discrete logarithm algorithm, which is employed in the key generation stage (i.e., off-line stage). Encryption and decryption (i.e., on-line stage) require only classical mechanisms and so are very efficient.

1.3 Related Works

1 [Quantum cryptography (QC)] The concept of *quantum cryptography* (QC), which utilizes a quantum channel and classical TMs (as well as a classical channel), was proposed by Bennet et al. [7, 6, 10, 9], and some protocols such as oblivious transfer based on this concept have also been presented [12, 8, 16, 29].

[1] We can also define adversaries based on the non-uniform model as quantum circuits [1, 19].

QC is one of the solutions to the above-mentioned problem when a QTM is realized in the future: that is, QC will be used for key-distribution in place of public-key encryption if a QTM is realized. The major difference between QC and QPKC is that QC employs a quantum channel (and classical channel) while QPKC employs only a classical channel. The security assumption for a QC scheme is quantum mechanics (believed by most physicists), while that for a QPKC scheme is a computational assumption (e.g., existence of a one-way function) in the QTM model.

Although several experimental QC systems have been already realized in the current technologies, recently reported security flaws of these systems are due to their realistic restrictions of quantum channels such as channel losses, realistic detection process, modifications of the qubits through channels, and fixed dark count error over long distance channels [11]. In addition, it is likely that much more complicated communication networks will be utilized in the future, and it seems technically very hard and much costly to realize a quantum channel from end to end through such complicated networks even in the future.

Accordingly, the QPKC approach seems much more promising, since in many applications encryption and key-distribution should be realized by end-to-end communication through (classical) complicated communication networks.

QC provides no solution to the problem of digital signatures when a QTM is realized: that is, QC cannot be used in digital signatures. Hence, our QPKC approach may be the only possible solution to the problem of digital signatures when a QTM is realized.

2 [Traditional public-key cryptosystems based on NP-hard problems] Many public-key cryptosystems based on NP-hard problems have been presented. These schemes were designed under the traditional public-key cryptosystem model (i.e., all parties are assumed to be classical Turing machines). If, however, such a scheme is also secure against QTM adversaries, it can be an example of our model, QPKC. This is because: the QPKC model allows us to employ the quantum mechanism for key generation, encryption, and decryption, but a PKC model, in which all parties but adversaries are classical TMs and only adversaries are QTMs, is still included in the QPKC model as a special case, since the classical TM is covered by QTM. Unfortunately, however, almost all existing public-key cryptosystems based on NP-hard problems have been broken, and the security of the unbroken systems often seems suspicious due to the lack of simplicity in the trapdoor tricks.

The advantage of our new paradigm, QPKC, over the traditional approach based on NP-hard problems is that quantum mechanisms are employed for key-generation, encryption, or decryption as well as adversaries. That is, we obtain new freedom in designing PKC because we can utilize a quantum mechanism for key-distribution and encryption/decryption. Actually, this paper shows a typical example, a knapsack-type scheme; its trapdoor trick is very simple and it looks much more secure than any knapsack-type scheme based on the traditional approach.

As for digital signatures, we can theoretically construct a concrete signature scheme based on any one-way function. This means that the scheme can be as secure as an NP-hard problem, if inverting the underlying one-way function is an NP-hard problem. Since such a construction is usually impractical, we believe that the QPKC approach will provide a way to construct an efficient signature scheme secure against QPT adversaries.

3 [Knapsack-type cryptosystems] The subset-sum (or subset-product) problems are typical NP-hard problems. Knapsack-type cryptosystems are based on theses problems.

The proposed scheme is a knapsack-type cryptosystem, and is closely related to the Merkle–Hellman "multiplicative" trapdoor knapsack scheme [30][2], and the Chor–Rivest scheme [13].

The Merkle–Hellman scheme was broken by Odlyzko [33] under some condition and has also been broken due to its low-density (asymptotically its density is zero). Typical realizations of the Chor–Rivest scheme were also cryptanalyzed by Schnorr–Hoerner and Vaudenay [36, 39], because of the known low cardinality of the subset-sum and the symmetry of the trapdoor information.

Note that these two schemes already use the trick of computing the discrete logarithm in the key-generation stage. Since they do not assume a quantum mechanism, the recommendation was to use a specific class of the discrete logarithm that could be easily computed by a classical machine.

Since we have freedom for selecting the underlying discrete logarithm problem, our scheme enjoys the use of more general mathematical tools than these two schemes. The proposed scheme employs the ring of integers, $\mathcal{O}_K$, of an algebraic number field, K, while the Merkle–Hellman scheme employs the ring of rational integer, $\mathbb{Z}$; the Chor–Rivest scheme employs the ring of polynomials over a finite field, $\mathbb{F}_p[x]$. The discrete logarithm in $\mathcal{O}_K/\mathfrak{p}$ should be computed in our scheme, while the discrete logarithms in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p[x]/(g(x))$ are computed, where $\mathfrak{p}$, p, and $g(x)$ are prime ideal, rational prime, and irreducible polynomial, respectively. All of them are discrete logarithms in finite fields.

Our scheme offers many advantages over these two schemes:

- No information on the underlying algebraic number field, K, in our scheme is revealed in the public-key, while it is publicly known that $\mathbb{Z}$ and $\mathbb{F}_p[x]$ are employed in the Merkle–Hellman and the Chor–Rivest schemes respectively. Here, note that there are exponentially many candidates from which K can be selected.
- No information on the underlying finite field is revealed in our scheme, while the underlying finite field is revealed in the Chor–Rivest scheme.

[2] Note that this scheme is different from the famous Merkle–Hellman knapsack scheme based on the super-increasing vector. Morii–Kasahara [31] and Naccache–Stern [32] also proposed a different type of multiplicative knapsack scheme, but their idea does not seem useful for our purpose since the scheme is vulnerable if the discrete logarithm is tractable.

– The density of a subset-sum problem in our scheme is at least 1, while that for the Merkle–Hellman scheme is asymptotically 0. If the parameters are chosen appropriately, the information rate in our scheme is asymptotically 1.

2 Quantum Public-Key Cryptosystems

This section defines quantum public-key cryptosystems (QPKCs) and related notions. These definitions are straightforwardly created from the classical definitions just by replacing a classical Turing machine (or classical circuits) with a quantum Turing machine (QTM) (or quantum circuits). Accordingly, this section defines only typical notions regarding QPKCs such as quantum one-way functions, quantum public-key encryption, and quantum digital signatures. We can easily extend the various classical security notions to the QPKC model.

Definition 1. *A function f is called* quantum one-way *(QOW) if the following two conditions hold:*

1. *[Easy to compute] There exists a polynomial time QTM, A, so that, on input x, A outputs $f(x)$ (i.e., $A(x)$=$f(x)$).*
2. *[Hard to invert] For every probabilistic polynomial time QTM, Adv, every polynomial $poly$, and all sufficiently large n,*

$$\Pr[Adv(f(x)) \in f^{-1}(f(x))] < 1/poly(n).$$

The probability is taken over the distribution of x, the (classical) coin flips of Adv, and quantum observation of Adv.

Note that all variables in this definition are classical strings, and no quantum channel between any pair of parties is assumed.

Remark: We can also define the *non-uniform* version of this notion, in which *Adv* is defined as polynomial size quantum circuits.[3] [1, 19]

Definition 2. *A* quantum public-key encryption *(QPKE) scheme consists of three probabilistic polynomial time QTMs, (G, E, D), as follows:*

1. *G is a probabilistic polynomial time QTM for generating keys. That is, G, on input 1^n, outputs (e, d) with overwhelming probability in n (taken over the classical coin flips and quantum observation of G), where e is a public-key, d is a secret-key, and n is a security parameter. (W.o.l.g., we suppose $|e| = |d| = n$.)*

[3] The concept of a quantum one-way function has been also presented by [19] independently from us. Our paper solves one of their open problems: find a candidate one-way function that is not classical one-way. The key generation function of our proposed scheme with input of a secret-key to output the corresponding public-key is such a candidate one-way function.

2. *E is an encryption function that produces ciphertext c, and D is a decryption function. For every message m of size $|m| = n$, every polynomial poly, and all sufficiently large n,*

$$\Pr[D(E(m, e), d) = m] > 1 - 1/poly(n).$$

The probability is taken over the (classical) coin flips and quantum observation of (G, E, D).

Note that all variables in this definition are classical strings, and no quantum channel between any pair of parties is assumed.

Remark: We omit the description of *security* in the above-mentioned definition, since we can naturally and straightforwardly extend the definitions of *one-wayness* (i.e., hard to invert $E(\cdot, e)$), *semantic security* [23] and *non-malleability* [4] to the QPKE model. In addition, passive and active adversaries (*adaptively chosen ciphertext attackers*) can be introduced for QPKE in the same manner as done for the classical PKE models [4]. The only difference between the classical and quantum security definitions is just that all adversaries are assumed to be probabilistic polynomial time QTMs (or polynomial size quantum circuits) in QPKC.

In addition, we can employ the random oracle model [2] to prove the security of QPKC schemes, since the random oracle model is generic and independent of the computation model. So, the conversions by Bellare–Rogaway [3] and Fujisaki–Okamoto [20, 21] are useful to enhance the security of the QPKE scheme proposed in this paper.

Definition 3. *A* quantum digital signature *(QDS) scheme consists of three probabilistic polynomial time QTMs, (G, S, V), as follows:*

1. *G is a probabilistic polynomial time QTM for generating keys. That is, G, on input 1^n, outputs (s, v) with overwhelming probability in n (taken over the classical coin flips and quantum observation of G), where s is a (secret) signing-key, v is a (public) verification-key, and n is a security parameter. (W.o.l.g., we suppose $|s| = |v| = n$.)*
2. *S is a signing function that produces signature σ, and V is a verification function. For every message m of size $|m| = n$, every polynomial poly, and all sufficiently large n,*

$$\Pr[(V(m, S(m, s), v) = 1] > 1 - 1/poly(n).$$

The probability is taken over the (classical) coin flips and quantum observation of (G, S, V).

Note that all variables in this definition are classical strings, and no quantum channel between any pair of parties is assumed.

Remark: Similarly to QPKE, we can naturally and straightforwardly extend the security definitions of *universal/existential unforgeability* and active adversaries (*adaptively chosen message attackers*) [24] to the QDS model.

3 Proposed Scheme

3.1 Basic Idea

The basic idea to realize QPKC is to employ an appropriate NP-hard problem as an intractable primitive problem, since the concept of QPKC is based on the assumption, NP-complete $\not\subseteq$ BQP. What is the most suitable NP-hard problem? We believe that the subset-sum (or subset-product) problem is one of the most suitable problems, since the algorithms to solve the subset-sum (or subset-product) problem and the ways to realize public-key cryptosystems based on this problem have been extensively studied for the last 20 years. Another promising candidate is the lattice problem, which seems to be closely related to the subset-sum problem.

There are two typical trapdoor tricks for subset-sum or subset-product problems. One is to employ super-increasing vectors for the subset-sum and prime factorization for the subset-product. Such a tractable trapdoor vector is transformed into a public-key vector, which looks intractable. However, almost all transformation tricks from a trapdoor subset-sum (or subset-product, resp.) vector to another subset-sum (or subset-product, resp.) vector have been cryptanalyzed due to their linearity and low density.

One promising idea for the transformation is, if computing a logarithm is feasible, to employ a non-linear transformation, exponentiation (and logarithm), that bridges the subset-sum and subset-product problems. To the best of our knowledge, two schemes have been proposed on this type of transformation: One is the Merkle–Hellman "multiplicative" trapdoor knapsack scheme [30], and the other is the Chor–Rivest scheme [13]. Unfortunately, typical realizations of these schemes have been cryptanalyzed.

To overcome the weakness of these schemes, the proposed scheme employs the ring of integers, $\mathcal{O}_K$, of an algebraic number field, K, which is randomly selected from exponentially many candidates. See Section 1.3 for a comparison with these two schemes.

3.2 Notation and Preliminaries

This section introduces notations and propositions on the algebraic number theory employed in this paper. Refer to some textbooks (e.g., [27, 28, 14]) for more details.

We denote an algebraic number field by K, the ring of integers of K by $\mathcal{O}_K$, and the norm of I by $\mathcal{N}(I)$. (In this paper, I is an integer or ideal of $\mathcal{O}_K$). We also denote the logarithm of n to the base 2 by $\log n$, and that to the base e by $\ln n$.

Before going to the description of our scheme, we present two propositions.

Proposition 1. *If K is a number field and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p}$ is a finite field, $\mathbb{F}_{p^f}$, and $\mathcal{N}(\mathfrak{p}) = p^f$. There exists an integral basis, $[\omega_1, \ldots, \omega_l]$, such that each residue class of $\mathcal{O}_K/\mathfrak{p}$ is uniquely represented by*

$$a_1\omega_1 + \cdots + a_l\omega_l,$$

where l is the degree of K, $0 \leq a_i < e_i (i = 1, \ldots, l)$, and $[e_1\omega_1, \cdots, e_n\omega_l]$ is an integral basis of $\mathfrak{p}$. Note that $\prod_{i=1}^{l} e_i = p^f$.

Here we note that, by using the HNF (Hermite Normal Form) representation of prime ideals, we can always assume that $\omega_1 = 1$, and $e_1 = p$. (For more detail, see Section 4.7 and Exercise 17 of [14].)

Note that $\mathcal{O}_K/\mathfrak{p}$ has some properties of integral domain and norm in addition to the structure of $\mathbb{F}_q$. These properties are specified by K and $\mathfrak{p}$. (In our scheme, the variety of the properties characterized by K and $\mathfrak{p}$ is utilized to enhance the security, since K and $\mathfrak{p}$ are concealed against adversaries and there are exponentially many candidates for K and $\mathfrak{p}$.)

The following proposition is a generalized version of Fermat's little theorem (obtained from the fact that $\mathcal{O}_K/\mathfrak{p}$ is a finite field, $\mathbb{F}_q$).

Proposition 2 (Fermat's little theorem). *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and a non-zero element g from $\mathcal{O}_K \backslash \mathfrak{p}$. Then we have*

$$g^{\mathcal{N}(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}.$$

Here, note that $\mathcal{O}_K$ is not always a unique factorization domain, although our decryption algorithm utilizes factorization of an element (integer) of $\mathcal{O}_K$.

3.3 Proposed scheme

Key generation

1. Fix a set $\mathcal{K}$ of algebraic number fields, available to the system.
2. Randomly choose an algebraic number field, K, from $\mathcal{K}$. Let $\mathcal{O}_K$ be its ring of integers.
3. Fix size parameters n, k from $\mathbb{Z}$.
4. Choose a prime ideal, $\mathfrak{p}$, of $\mathcal{O}_K$, and randomly choose an element, g, of $\mathcal{O}_K$ such that g is a generator of the multiplicative group of finite field $\mathcal{O}_K/\mathfrak{p}$. Here, an element in $\mathcal{O}_K/\mathfrak{p}$ is uniquely represented by basis $[1, \omega_2, \ldots, \omega_l]$ and integer tuple $(e_1, e_2, \ldots, e_l)$ (where $e_1 = p$) defined by Proposition 1. That is, for any $x \in \mathcal{O}_K$, there exist rational integers $x_1, x_2, \ldots, x_l \in \mathbb{Z}$ $(0 \leq x_i < e_i)$ such that $x \equiv x_1 + x_2\omega_2 + \cdots + x_l\omega_l \pmod{\mathfrak{p}}$. Note that p is the rational prime below $\mathfrak{p}$.
5. Choose n integers $p_1, \ldots, p_n$ from $\mathcal{O}_K/\mathfrak{p}$ with the condition that $\mathcal{N}(p_1), \ldots, \mathcal{N}(p_n)$ are co-prime, and for any subset $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ from $\{p_1, p_2, \ldots, p_n\}$, there exist rational integers $a_1, a_2, \ldots, a_l$ $(0 \leq a_i < e_i)$ such that $\prod_{j=1}^{k} p_{i_j} = a_1 + a_2\omega_2 + \cdots + a_l\omega_l$.
6. Use Shor's algorithm for finding discrete logarithms to get $a_1, \ldots, a_n$ such that
$$p_i \equiv g^{a_i} \pmod{\mathfrak{p}},$$
where $a_i \in \mathbb{Z}/(\mathcal{N}(\mathfrak{p}) - 1)\mathbb{Z}$, and $1 \leq i \leq n$.
7. Randomly choose a rational integer, d, in $\mathbb{Z}/(\mathcal{N}(\mathfrak{p}) - 1)\mathbb{Z}$.
8. Compute $b_i = (a_i + d) \bmod (\mathcal{N}(\mathfrak{p}) - 1)$ for each $1 \leq i \leq n$.
9. The public key is $(\mathcal{K}, n, k, b_1, b_2, \ldots, b_n)$, and the private key is $(K, g, d, \mathfrak{p}, p_1, p_2, \ldots, p_n)$.

Encryption

1. Fix the length of plaintext M to $\lfloor \log \binom{n}{k} \rfloor$.
2. Encode M into a binary string $m = (m_1, m_2, \ldots, m_n)$ of length n and of Hamming weight k (i.e., of having exactly k 1's) as follows:
   (a) Set $l \leftarrow k$.
   (b) For i from 1 to n do the following:
   If $M \geq \binom{n-i}{l}$ then set $m_i \leftarrow 1$, $M \leftarrow M - \binom{n-i}{l}$, $l \leftarrow l - 1$. Otherwise, set $m_i \leftarrow 0$. (Notice that $\binom{l}{0} = 1$ for $l \geq 0$, and $\binom{0}{l} = 0$ for $l \geq 1$.)
3. Compute ciphertext c by
$$c = \sum_{i=1}^{n} m_i b_i.$$

Decryption

1. Compute $r = (c - kd) \bmod (\mathcal{N}(\mathfrak{p}) - 1)$.
2. Compute
$$u \equiv g^r \pmod{\mathfrak{p}}.$$
3. Find m as follows: If $p_i \mid u$ then set $m_i \leftarrow 1$. Otherwise, set $m_i \leftarrow 0$. After completing this procedure for all p_i's ($1 \leq i \leq n$), set $m = (m_1, \ldots, m_n)$.
4. Decode m to plaintext M as follows:
   (a) Set $M \leftarrow 0$, $l \leftarrow k$.
   (b) For i from 1 to n do the following:
   If $m_i = 1$, then set $M \leftarrow M + \binom{n-i}{l}$ and $l \leftarrow l - 1$.

3.4 Correctness and remarks

1 [Decryption] We show that decryption works. We observe that

$$\begin{aligned} u \equiv g^r \equiv g^{c-kd} \equiv g^{(\sum_{i=1}^{n} m_i b_i) - kd} \equiv g^{\sum_{i=1}^{n} m_i a_i} \pmod{\mathfrak{p}} \\ \equiv \prod_{i=1}^{n} (g^{a_i})^{m_i} \pmod{\mathfrak{p}} \\ \equiv \prod_{i=1}^{n} p_i^{m_i} \pmod{\mathfrak{p}} \\ = \prod_{i=1}^{n} p_i^{m_i}, \end{aligned}$$

since, from the condition of $(p_1, \ldots, p_n)$, $\prod_{i=1}^{n} p_i^{m_i}$ can be represented by $a_1 + a_2\omega_2 + \cdots + a_l\omega_l$ for some rational integers $a_1, a_2, \ldots, a_l$ ($0 \leq a_i < e_i$).

Since $\mathcal{O}_K$ is not always a unique factorization domain, we select $p_1, \ldots, p_n$ so that $\mathcal{N}(p_1), \ldots, \mathcal{N}(p_n)$ are co-prime. It follows that a product of $p_1, \ldots, p_n$ is uniquely factorized if we use only these elements as factors. Thus, a ciphertext is uniquely deciphered if a product of $p_1, \ldots, p_n$ is correctly recovered.

2 [Number fields] Considering efficiency and security, a typical example for $\mathcal{K}$ is the set of quadratic fields, $\{\mathbb{Q}(\sqrt{D})\}$. Especially, the set of imaginary quadratic fields is strongly recommended as $\mathcal{K}$ (see Appendix 2 for how to select parameters). Even in this set $\mathcal{K} = \{\mathbb{Q}(\sqrt{-D})\}$ of fields, there are exponentially many candidates.

3 [Special Parameters] Although the parameters of the imaginary quadratic fields for our scheme are described in Appendix 2, we will now show another way to select parameters, $(p_1, p_2, \ldots, p_n)$, for more general fields. Rational primes, $p_1, p_2, \ldots, p_n$, are selected such that $\prod_{j=1}^{k} p_{i_j} < e_1 = p$ for any subset $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ from $\{p_1, p_2, \ldots, p_n\}$. In that case, for any subset $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ from $\{p_1, p_2, \ldots, p_n\}$, there exists a rational integer a_1 ($0 < a_1 < e_1$) such that $\prod_{j=1}^{k} p_{i_j} = a_1$. That is, $\prod_{j=1}^{k} p_{i_j}$ can be represented by $\prod_{j=1}^{k} p_{i_j} = a_1\omega_1 + \cdots + a_l\omega_l$, where $a_2 = \cdots = a_l = 0$. Here we note that, by using the HNF (Hermite Normal Form) representation of prime ideals, we can always assume that $\omega_1 = 1$, and $e_1 > 1$ (For more detail, see Section 4.7 and Exercise 17 of [14]).

The shortcoming of this case is that $\prod_{j=1}^{k} p_{i_j} < e_1 = p = (\mathcal{N}(\mathfrak{p}))^{1/f}$, when $\mathcal{N}(\mathfrak{p})) = p^f$. Then the density and rate should be smaller (the density is about $\frac{n}{fk\log n}$, and the rate is about $\frac{k\log n - k\log k}{fk\log n}$) when f is greater than 1. (Note that $\prod_{j=1}^{k} p_{i_j} \approx \mathcal{N}(\mathfrak{p})$, in the case of Appendix 2: imaginary quadratic fields.) See below for a discussion of density and rate.

4 [Density and rate] Here we estimate the density and rate in the case of Appendix 2. (see Section 3.5 for the definition of density and information rate.)

The size of b_i (i.e., $|b_i|$) is $|\mathcal{N}(\mathfrak{p})|$, $k \times |\mathcal{N}(p_i)| \approx |\mathcal{N}(\mathfrak{p})|$, and $|\mathcal{N}(p_i)| \approx 2\log n$. Accordingly, ignoring a minor term, we obtain $|b_i| \approx |\mathcal{N}(\mathfrak{p})| \approx 2k\log n$. Hence the density D of our scheme is estimated by $\frac{n}{2k\log n}$, and the rate R by $\frac{k\log n - k\log k}{2k\log n}$. If $k = 2^{(\log n)^c}$ for a constant $c < 1$, the information rate, R, is asymptotically $1/2$, and density, D, is asymptotically ∞.

5 [Shor's algorithm] Key generation uses Shor's algorithm for finding discrete logarithms. The scope of Shor's original algorithm is for multiplicative cyclic groups. In particular, given a rational prime p, a generator g of the group $(\mathbb{Z}/p\mathbb{Z})^\times$, and a target rational integer x from $(\mathbb{Z}/p\mathbb{Z})^\times$, Shor's algorithm can find a rational integer a from $\mathbb{Z}/(p-1)\mathbb{Z}$ such that

$$g^a = x \bmod p.$$

Shor's algorithm basically uses three registers. The first and the second registers are for all of the rational integers from 0 to q where q is, roughly, a large rational integer, and the third is for $g^a x^{-b} \bmod p$. Our scheme only needs to change the contents in the third register to

$$g^a p_i^{-b} \bmod \mathfrak{p}.$$

Since each of these contents can be computed efficiently even by classical computers, we can find the discrete logarithms in our scheme.

6 [Coding] We next mention about the encoding scheme used in encryption and decryption. This scheme is well known in combinatorial literature. (see [15]. This scheme is also employed by the Chor–Rivest cryptosystem.) This encoding scheme is used mainly for avoiding the low-density attacks mentioned later.

7 [Complexity] Here we mention about the time complexity needed for the key generation as well as the encryption and the decryption. The most difficult part in the key generation is the computation of discrete logarithms at line 6. In particular, we compute n discrete logarithms $a_1, \ldots, a_n$ in field $\mathcal{O}_K/\mathfrak{p}$. For the encryption, once we get the encoded string by line 2 in the encryption, all we need is to add k integer, each smaller than $\mathcal{N}(\mathfrak{p})$. For the decryption, we perform the modular exponentiation $g^r \bmod \mathfrak{p}$ in line 2. This dominates the running time of the decryption. Raising a generator g to a power in the range up to $\mathcal{N}(\mathfrak{p})$ takes at most $2 \times \log \mathcal{N}(\mathfrak{p})$ modular multiplications by using a standard multiplication technique.

3.5 Security Consideration

We provide an initial analysis for the security of our scheme by considering several possible attack approaches.

We can use quantum computers also for attacks in our setting. As far as we know, despite recent attempts at designing efficient quantum algorithms for problems where no efficient classical probabilistic algorithm is known, all known such quantum algorithms are for some special cases of the hidden subgroup problem. Let f be a function from a finitely generated group G_1 to a finite set such that f is constant on the cosets of a subgroup G_2. Given a way of computing f, a hidden subgroup problem is to find G_2 (i.e., a generating set for G_2). The problems of factoring and finding discrete logarithms can be formulated as instances of the hidden subgroup problems.

There is also a result by Grover [25] for database search. He shows that the problem of finding an entry with the target value can be searched in $O(\sqrt{N})$ time, where N is the number of entries in the database. This result implies NP-complete problems can be solved in $O(\sqrt{N})$ time.

However, if we do not put a structure in the database, i.e., we need to ask oracles for the contents in the database, it is known that we cannot make algorithms whose time complexity is $o(\sqrt{N})$. Thus, it is widely believed that NP-complete problems cannot be solved in polynomial time even with quantum computers.

Finding secret keys from public keys Recall that we have the public key $(\mathcal{K}, n, k, b_1, b_2, \ldots, b_n)$, and the secret key $(K, g, d, \mathfrak{p}, p_1, p_2, \ldots, p_n)$, where

$$p_i \equiv g^{a_i} \pmod{\mathfrak{p}},$$

and $b_i = (a_i + d) \bmod (\mathcal{N}(\mathfrak{p}) - 1)$. In a passive attack setting, the attacker has only information on the public key. The information on n and k only exposes problem size.

Assume we choose exponentially large $\mathcal{K}$. First, K seems to be impossible to guess, since we have exponentially large possibilities for K. Second, g and d would be hard to guess, even if K is revealed. This is again because we have exponentially large possibilities for them.

Third, if K is revealed, we could guess only a subset of p_i's, since we have chosen roughly n prime elements out of cn ones, where c is a constant. Suppose we find a subset of p_i's. In order to use them in the attack by Odlyzko for multiplicative-knapsack [33], the size of the subset must be fairly large. In addition, it is necessary to find the correspondences between the elements of the subset and b_i's. Here we observe that b_i's seem to be random because of the discrete-log relation in our function. Thus, it seems impossible for any reasonable relation between public keys and private keys to be made without knowing K, g, d, and $\mathfrak{p}$, so the critical attacks of directly finding public keys from secret keys seem to be difficult.

Notice that, in contrast to our scheme, the Chor–Rivest cryptosystem exposes the information corresponding to K, p_i's, and q of the underlying $\mathbb{F}_q$ in the public key, which enables the attackers to make use of the symmetry of the secret keys (see [39]).

Finding plaintexts from ciphertexts For many knapsack-type cryptosystems, low-density attacks are known to be effective. Thus, they might be effective against our scheme. A low-density attack finds plaintexts from ciphertexts by directly solving feasible solutions to the subset sum problems that the cryptosystem is based on.

The subset-sum problem is, given positive rational integers c and $a_1, \ldots, a_n$ to solve the equation $c = \sum_{i=1}^{n} m_i a_i$ with each $m_i \in \{0, 1\}$. Let $a = \{a_1, \ldots, a_n\}$. The density $d(a)$ of a knapsack system is defined to be $d(a) = \frac{n}{\log(\max_i a_i)}$. Density is an approximate measure of the information rate for knapsack-type cryptosystems. The shortest vector in a lattice solves almost all subset sum problems whose density is less than 0.9408 [35]. If we choose appropriate parameters for our scheme, the density is at least 1 (see Section 3.4).

It is known that the algorithms for finding the shortest vector in a lattice can be used to find the solutions to the subset sum problems. The LLL algorithm plays an important role in this kind of attack. However, it is not known that the LLL algorithm can be improved with the quantum mechanism. Incidentally, as far as we know, for any approximation algorithm, it is not known that its approximation ratio can be improved by the addition of the quantum mechanism.

Information rate R is defined to be $\frac{\log |M|}{N}$, where $|M|$ is the size of message space and N is the number of bits in a cipher text. If we select appropriate parameters, the information rate of our scheme is about $1/2$ (see Section 3.4).

Notice again here that it is widely believed that NP-complete problems cannot be solved efficiently even with quantum computers. Since the subset-sum

problem is a typical NP-complete problem, our scheme with appropriate parameters does not seem to be open to successful crucial attacks that find plaintexts from ciphertexts even if quantum computers are used.

4 Extensions

We can extend our QPKC model to more general ones. One possible extension is to relax the restriction of variables employed inside QTMs to quantum strings. For example, a secret key of QPKE or QDS can be a quantum string (qubits) stored in a quantum register. The other possible extension is to use quantum channels as well as QTMs and classical channels. However, these extensions are beyond the scope of this paper.

Another direction in extension is to extend the computational model to other non-classical models such as DNA computers.

5 Conventional PKC Version

Our techniques to construct QPKC schemes using knapsack problems can be also employed to realize standard (non-quantum) public-key encryption based on conventional (non-quantum) algorithms [34]. We utilize the Chinese remainder theorem technique in the key generation procedure to compute the discrete logarithm very efficiently even if conventional (non-quantum) algorithms are used. In our construction, the secrecy of the underlying field, K, still guarantees its security.

6 Concluding Remarks

This paper presented a new paradigm of cryptography, quantum public-key cryptosystems (QPKCs), which consist of quantum public-key encryption (QPKE) and quantum digital signatures (QDSs). It also proposed a concrete scheme for quantum public-key cryptosystems, that will be very efficient if a QTM is realized.

The situation of this paper is comparable to that in the late 1970's, when many new ideas were proposed to realize Diffie–Hellman's paradigm. Almost all trials such as the so-called knapsack cryptosystems based on subset-sum and subset-product problems failed, and only the schemes based on integer factoring and discrete logarithm problems are still alive and widely employed.

The main purpose of this paper is to explicitly raise the concept of quantum public-key cryptosystems and to encourage researchers to create and cryptanalyze concrete QPKC schemes to investigate the feasibility of this concept.

There are many open problems regarding this concept as follows:

1. Find attacks on our QPKE scheme. (In particular, as an initial trial, cryptanalyze a restricted version of our scheme, where the underlying algebraic number field, K, is published and limited to the rational number field, $\mathbb{Q}$ (See Appendix 1)).

2. Find (indirect) evidence that a one-way function exists in the QTM model, or show that NP $\not\subseteq$ BQP under a reasonable assumption.
3. Realize a concrete quantum digital signature (QDS) scheme.
4. Extend the concept of QPKC (see Section 4).
5. Realize QPKC schemes based on various NP-hard problems.
6. Realize QPKC schemes that employ Shor's factoring algorithm or Grover's database search algorithm.

References

1. Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D. P., Margolus, N., Shor, P., Sleator, T., Smolin, J., and Weinfurter, H. Elementary Gates for Quantum Computation. *Physical Review A 52*, 5 (Nov. 1995), 3457–3467.
2. Bellare, M., and Rogaway, P. Entity authentication and key distribution. In *Advances in Cryptology—CRYPTO '93* (22–26 Aug. 1993), D. R. Stinson, Ed., vol. 773 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 232–249.
3. Bellare, M., and Rogaway, P. Optimal Asymmetric Encryption—How to Encrypt with RSA. In *Advances in Cryptology—EUROCRYPT'94* (1994), pp. 92–111.
4. Bellare, M., Desai, A., Pointcheval, D., and Rogaway, P. Relations among Notions of Security for Public-Key Encryption Schemes. In *Advances in Cryptology—CRYPTO'98* (1998), pp. 26–45.
5. Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. Strengths and weaknesses of quantum computing. *SIAM J. Comput. 26*, 5 (Oct. 1997), 1510–1523.
6. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. Experimental quantum cryptography. *Journal of Cryptology 5*, 1 (1992), 3–28.
7. Bennett, C. H., and Brassard, G. An update on quantum cryptography. In *Advances in Cryptology: Proceedings of CRYPTO 84* (19–22 Aug. 1984), G. R. Blakley and D. Chaum, Eds., vol. 196 of *Lecture Notes in Computer Science*, Springer-Verlag, 1985, pp. 475–480.
8. Bennett, C. H., Brassard, G., Crépeau, C., and Skubiszewska, M.-H. Practical quantum oblivious transfer. In *Advances in Cryptology—CRYPTO '91* (11–15 Aug. 1991), J. Feigenbaum, Ed., vol. 576 of *Lecture Notes in Computer Science*, Springer-Verlag, 1992, pp. 351–366.
9. Bennett, C. H., Brassard, G., and Ekert, A. K. Quantum cryptography. *Scientific America 262*, 10 (Oct. 1992), 26–33.
10. Bennett, C. H., Brassard, G., and Mermin, N. D. Quantum cryptography without Bell's theorem. *Physical Review Letters 68*, 5 (Feb. 1992), 557–559.
11. Brassard, G., Lütkenhaus, N., Tal, M., and Sanders, B. C. Security Aspects of Practical Quantum Cryptography. In *Advances in Cryptology—EUROCRYPT2000* (2000), pp. 289–299.
12. Brassard, G., and Crépeau, C. Quantum bit commitment and coin tossing protocols. In *Advances in Cryptology—CRYPTO '90* (11–15 Aug. 1990), A. J. Menezes and S. A. Vanstone, Eds., vol. 537 of *Lecture Notes in Computer Science*, Springer-Verlag, 1991, pp. 49–61.
13. Chor, B., and Rivest, R. L. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Trans. on Information Theory 34* (1988), 901–909.
14. Cohen, H. *A Course in Computational Algebraic Number Theory.* Springer, 1993.

15. Cover, T. M. Enumerative source encoding. *IEEE Trans. on Information Theory IT-19* (1973), 901–909.
16. Crépeau, C., and Salvail, L. Quantum oblivious mutual identification. In Guillou and Quisquater [26], pp. 133–146.
17. Deutsch, D., and Jozsa, R. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A 439* (1992), 553–558.
18. Diffie, W., and Hellman, M. New directions in cryptography. *IEEE Trans. on Information Theory IT-22*, 6 (1976), 644–654.
19. Dumais, P., Mayers, D., and Salvail, L. Perfectly Concealing Quantum Bit Commitment from any Quantum One-Way Permutation. In *Advances in Cryptology—EUROCRYPT2000* (2000), pp. 300–315.
20. Fujisaki, E. and Okamoto, T. How to Enhance the Security of Public-Key Encryption at Minimum Cost. In *PKC'99* (1999), pp. 53–68.
21. Fujisaki, E. and Okamoto, T. Secure Integration of Asymmetric and Symmetric Encryption Schemes. In *Advances in Cryptology—CRYPTO'99* (1999), pp. 537–554.
22. Goldreich, O. On the foundations of modern cryptography. In *Advances in Cryptology—CRYPTO '97* (17–21 Aug. 1997), B. S. Kaliski Jr., Ed., vol. 1294 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 46–74.
23. Goldwasser, S., and Micali, S. Probabilistic encryption. *J. Comput. Syst. Sci. 28*, 2 (Apr. 1984), 270–299.
24. Goldwasser, S., Micali, S., and Rivest, R. L. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput. 17*, 2 (Apr. 1988), 281–308.
25. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing* (Philadelphia, Pennsylvania, 22–24 May 1996), pp. 212–219.
26. Guillou, L. C., and Quisquater, J.-J., Eds. *Advances in Cryptology—EUROCRYPT 95* (21–25 May 1995), vol. 921 of *Lecture Notes in Computer Science*, Springer-Verlag.
27. Lang, S. *Algebraic Number Theory, Second Edition*, Springer, 1994.
28. Marcus, D. A. *Number Fields*, Springer, 1977.
29. Mayers, D. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology—CRYPTO '96* (18–22 Aug. 1996), N. Koblitz, Ed., vol. 1109 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 343–357.
30. Merkle, R. C., and Hellman, M. E. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. on Information Theory 24* (1978), 525–530.
31. Morii, M., and Kasahara, M. New Public Key Cryptosystem Using Discrete Logarithms over $GF(p)$. *Trans. of the IEICE J71-D*, 2 (Feb. 1988), 448–453 (In Japanese).
32. Naccache, D., and Stern, J. A New Public-Key Cryptosystem. In *Advances in Cryptology—EUROCRYPT'97* (1997), pp. 27–36.
33. Odlyzko, A. M. Cryptanalytic attacks on the multiplicative knapsack cryptosystem and on Shamir's fast signature scheme. *IEEE Trans. on Information Theory IT-30* (1984), 594–601.
34. Okamoto, T., and Tanaka, K. A New Approach to Knapsack Cryptosystems. manuscript (2000).
35. Orton, G. A Multiple-Iterated Trapdoor for Dense Compact Knapsacks. In *Advances in Cryptology—EUROCRYPT'94* (1994), pp. 112–130.
36. Schnorr, C. P., and Hörner, H. H. Attacking the Chor–Rivest cryptosystem by improved lattice reduction. In Guillou and Quisquater [26], pp. 1–12.

37. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput. 26*, 5 (Oct. 1997), 1484–1509.
38. Simon, D. R. On the power of quantum computation. *SIAM J. Comput. 26*, 5 (Oct. 1997), 1474–1483.
39. Vaudenay, S. Cryptanalysis of the Chor–Rivest cryptosystem. In *Advances in Cryptology—CRYPTO'98* (1998), pp. 243–256.

Appendix 1: Restricted Version for Explaining Our Scheme

This section presents a very restricted version of our scheme in order to help readers to understand our scheme more easily. Since this version seems to be much less secure than the full version, we do not recommend this version for practical usage, although we have not found any effective attack even against this restricted version.

Suppose that we set $\mathcal{K} = \{\mathbb{Q}\}$. i.e., we have only the field $\mathbb{Q}$ of rational numbers for the system. Then, the ring $\mathcal{O}_K$ of integers of $\mathbb{Q}$ is $\mathbb{Z}$. In this section, we use a *prime* to refer to a rational prime, and an *integer* a rational integer. The restricted version of our scheme is as follows:

Key generation

1. Fix size parameters n, k from $\mathbb{Z}$.
2. Randomly choose a prime p, a generator g of the group $(\mathbb{Z}/p\mathbb{Z})^\times$, and n co-primes $p_1, \ldots, p_n \in \mathbb{Z}/p\mathbb{Z}$ such that $\prod_{j=1}^{k} p_{i_j} < p$ for any subset $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ from $\{p_1, p_2, \ldots, p_n\}$.
3. Use Shor's algorithm for finding discrete logarithms to get integers $a_1, \ldots, a_n \in \mathbb{Z}/(p-1)\mathbb{Z}$ satisfying $p_i \equiv g^{a_i} \pmod{p}$, for each $1 \le i \le n$.
4. Randomly choose a integer $d \in \mathbb{Z}/(p-1)\mathbb{Z}$.
5. Compute $b = (a_i + d) \bmod (p-1)$, for each $1 \le i \le n$.
6. The public key is $(n, k, b_1, b_2, \ldots, b_n)$, and the secret key is $(g, d, p, p_1, p_2, \ldots, p_n)$.

Encryption

1. Fix the length of plaintext M to $\lfloor \log \binom{n}{k} \rfloor$.
2. Encode M into a binary string $m = (m_1, m_2, \ldots, m_n)$ of length n and Hamming weight k (i.e., having exactly k 1's) as follows:
   (a) Set $l \leftarrow k$.
   (b) For i from 1 to n do the following:
   If $M \ge \binom{n-i}{l}$ then set $m_i \leftarrow 1$, $M \leftarrow M - \binom{n-i}{l}$, $l \leftarrow l - 1$. Otherwise, set $m_i \leftarrow 0$. (Notice that $\binom{l}{0} = 1$ for $l \ge 0$, and $\binom{0}{l} = 0$ for $l \ge 1$.)
3. Compute the ciphertext c by $c = \sum_{i=1}^{n} m_i b_i$.

Decryption

1. Compute $r = (c - kd) \bmod (p-1)$.
2. Compute $u = g^r \bmod q$.
3. Find the factors of u. If p_i is a factor, then set $m_i \leftarrow 1$. Otherwise, $m_i \leftarrow 0$.
4. Decode m to the plaintext M as follows:
   (a) Set $M \leftarrow 0$, $l \leftarrow k$.
   (b) For i from 1 to n do the following:
   If $m_i = 1$, then set $M \leftarrow M + \binom{n-i}{l}$ and $l \leftarrow l - 1$.

Appendix 2: Imaginary Quadratic Field Version of Our Scheme

This section presents the imaginary quadratic field version of our scheme. Before describing the proposed scheme, we will briefly review basic results of the arithmetic on imaginary quadratic fields and present a proposition.

Imaginary Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field of discriminant $-D$. Here we note that the ring of integers, $\mathcal{O}_K$, of K has an integral basis $[1, \omega]$, where $\omega = \sqrt{-D/4}$ (if $-D \equiv 0 \pmod 4$), $\omega = \frac{1+\sqrt{-D}}{2}$ (otherwise), and this called the standard basis of $\mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ of residue degree f, namely, $\mathcal{N}(\mathfrak{p}) = p^f$, where p is a rational prime integer below $\mathfrak{p}$. Then we can take an integral basis of $\mathfrak{p}$ as $[p, e_2\omega_2]$, where $e_2 = p^{f-1}$, and $\omega_2 = b+\omega$ with some rational integer b (e.g. if $-D \equiv 0 \pmod 4$ and $-D$ is a quadratic residue $\bmod p$, then b is a root of $b^2 \equiv -D \pmod p$). We also call this basis the standard basis of $\mathfrak{p}$. Then, each residue class of $\mathcal{O}_K/\mathfrak{p}$ is uniquely represented by $x_1 + x_2\omega_2$, where $-p/2 < x_1 < p/2$ and $-e_2/2 < x_2 < e_2/2$ (cf. Proposition 1). From here, we fix a complete representative system of $\mathcal{O}_K/\mathfrak{p}$ as follows:

$$R(\mathfrak{p}) = \{x_1 + x_2\omega_2 \in \mathcal{O}_K \mid -p/2 < x_1 < p/2, -e_2/2 < x_2 < e_2/2\}.$$

We then have the following proposition.

Proposition 3. *Let $K = \mathbb{Q}(\sqrt{-D})$ be an imaginary quadratic field of discriminant $-D$, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ with $\mathcal{N}(\mathfrak{p}) = p^f$, where $f = 1, 2$. Let $[1, \omega]$ and $[p, e_2\omega_2]$ be the standard basis of $\mathcal{O}_K$ and $\mathfrak{p}$, respectively.*

Then

1. *Case: $\mathcal{N}(\mathfrak{p}) = p$ ($f = 1$)*
   For any integer $x = x_1 + x_2\omega_2 \in \mathcal{O}_K$, if it satisfies $\mathcal{N}(x) < p^2/4$ and $x_2 = 0$, then we have $x \in R(\mathfrak{p})$. In this case, we can take $R(\mathfrak{p})$ as $\{x \in \mathbb{Z} \mid -p/2 < x < p/2\}$.
2. *Case: $\mathcal{N}(\mathfrak{p}) = p^2$ ($f = 2$)*
   For any integer $x = x_1 + x_2\omega_2 \in \mathcal{O}_K$, if $-D \equiv 0 \pmod 4$ and $\mathcal{N}(x) < p^2/4$, then we have $x \in R(\mathfrak{p})$, while if $-D \equiv 1 \pmod 4$ and $\mathcal{N}(x) < \frac{(p-1)^2 D}{4(1+D)}$, then we have $x \in R(\mathfrak{p})$.

Proof. In the case of $f = 1$, $x = x_1 + x_2\omega_2 \in R(\mathfrak{p})$ if and only if $x_1^2 < p^2/4$ and $x_2 = 0$, namely, $\mathcal{N}(x) < p^2/4$ and $x_2 = 0$. For the case of $f = 2$ and $-D \equiv 0 \pmod 4$, it is sufficient to show that $\{(x_1, x_2) \in \mathbb{Z}^2 \mid x_1 + x_2\omega_2 \in R(\mathfrak{p})\}$ contains $\{(x_1, x_2) \in \mathbb{Z}^2 \mid x_1^2 + \frac{D}{4}x_2^2 < \frac{p^2}{4}\}$. Note that we can take $b = 0$ in the standard basis, namely, $\omega_2 = \omega = \sqrt{-D/4}$ and $e_2 = p$. Similarly, for the case of $f = 2$ and $-D \equiv 2, 3 \pmod 4$, it is sufficient to show that $\{(s, t) \in \mathbb{Z}^2 \mid -3p/2 < s < 3p/2, -p/2 < t < p/2, s \equiv t \pmod 2\}$ contains $\{(s, t) \in \mathbb{Z}^2 \mid s^2 + Dt^2 < \frac{D(p-1)^2}{1+D}, s \equiv t \pmod 2\}$. By drawing pictures, we can easily show these relationships.

Proposed Scheme

We will now present our proposed scheme using imaginary quadratic fields.

Key generation

1. Fix a set $\mathcal{K}$ of imaginary quadratic fields, available to the system.
2. Randomly choose an imaginary quadratic field, $K = \mathbb{Q}(\sqrt{-D})$, where $-D$ is the discriminant of K, from $\mathcal{K}$. Let $\mathcal{O}_K$ be the ring of integers of K.
3. Fix size parameters n, k from $\mathbb{Z}$.
4. Choose a prime ideal, $\mathfrak{p}$, of degree 2 from $\mathcal{O}_K$, and randomly choose an element, g, of $\mathcal{O}_K$ such that g is a generator of the multiplicative group of finite field $\mathcal{O}_K/\mathfrak{p}$. Here, an element in $\mathcal{O}_K/\mathfrak{p}$ is uniquely represented by basis $[1, \omega_2]$ and integer pair (p, p). That is, for any $x \in \mathcal{O}_K$, there exist integers $x_1, x_2 \in \mathbb{Z}$, $-p/2 < x_1, x_2 < p/2$ such that $x \equiv x_1 + x_2\omega_2 \pmod{\mathfrak{p}}$.
5. Choose n integers $p_1, \ldots, p_n$ from $\mathcal{O}_K/\mathfrak{p}$ with the condition that $\mathcal{N}(p_1), \ldots, \mathcal{N}(p_n)$ are co-prime, and for any subset $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ from $\{p_1, p_2, \ldots, p_n\}$, if $-D \equiv 0 \pmod 4$, $\prod_{j=1}^{k} \mathcal{N}(p_{i_j}) < \frac{p^2}{4}$, otherwise, $\prod_{j=1}^{k} \mathcal{N}(p_{i_j}) < \frac{(p-1)^2 D}{4(1+D)}$.
6. Use Shor's algorithm for finding discrete logarithms to get $a_1, \ldots, a_n$ such that
$$p_i \equiv g^{a_i} \pmod{\mathfrak{p}},$$
where $a_i \in \mathbb{Z}/(\mathcal{N}(\mathfrak{p}) - 1)\mathbb{Z}$, and $1 \le i \le n$.
7. Randomly choose a rational integer, d, in $\mathbb{Z}/(\mathcal{N}(\mathfrak{p}) - 1)\mathbb{Z}$.
8. Compute $b_i = (a_i + d) \bmod (\mathcal{N}(\mathfrak{p}) - 1)$ for each $1 \le i \le n$.
9. The public key is $(\mathcal{K}, n, k, b_1, b_2, \ldots, b_n)$, and the private key is $(K = \mathbb{Q}(\sqrt{-D}), g, d, \mathfrak{p}, p_1, p_2, \ldots, p_n)$.

Encryption

1. Fix the length of plaintext M to $\lfloor \log \binom{n}{k} \rfloor$.
2. Encode M into a binary string $m = (m_1, m_2, \ldots, m_n)$ of length n and of Hamming weight k (i.e., of having exactly k 1's) as follows:
   (a) Set $l \leftarrow k$.

(b) For i from 1 to n do the following:
If $M \geq \binom{n-i}{l}$ then set $m_i \leftarrow 1$, $M \leftarrow M - \binom{n-i}{l-1}$, $l \leftarrow l-1$. Otherwise, set $m_i \leftarrow 0$. (Notice that $\binom{l}{0} = 1$ for $l \geq 0$, and $\binom{0}{l} = 0$ for $l \geq 1$.)

3. Compute ciphertext c by $c = \sum_{i=1}^{n} m_i b_i$.

Decryption

1. Compute $r = (c - kd) \bmod (\mathcal{N}(\mathfrak{p}) - 1)$.
2. Compute $u \equiv g^r \pmod{\mathfrak{p}}$.
3. Find m as follows:
   (a) Let $[1, \omega_2]$ and (p, p) be the basis and integer pair defined by Proposition 1. From the selection of $p_1, \ldots, p_n$, u can be represented by $u = a_1 + a_2\omega_2$ for some integers $a_1, a_2 \in \mathbb{Z}$ with $-p/2 < a_i < p/2$ $(i = 1, 2)$.
   (b) Do the following:
   If $p_i \mid u$ then set $m_i \leftarrow 1$. Otherwise, set $m_i \leftarrow 0$. After completing this procedure for all p_i's $(1 \leq i \leq n)$, set $m = (m_1, \cdots, m_n)$.
4. Decode m to plaintext M as follows:
   (a) Set $M \leftarrow 0$, $l \leftarrow k$.
   (b) For i from 1 to n do the following:
   If $m_i \leftarrow 1$, then set $M \leftarrow M + \binom{n-i}{l}$ and $l \leftarrow l - 1$.

Remark 1: Note that we can easily choose a prime ideal, $\mathfrak{p}$, of degree 2 as follows: choose any rational prime, p, such that $-D$ is a quadratic non-residue mod$p$, then set $\mathfrak{p} = p\mathcal{O}_K$. In other words, p is also a prime element in $\mathcal{O}_K$. Furthermore, it can be efficiently checked whether p is a prime in $\mathcal{O}_K$ or not by computing the Legendre symbol, $\left(\frac{-D}{p}\right)$, namely p is a prime element in $\mathcal{O}_K$ if and only if $\left(\frac{-D}{p}\right) = -1$, and always selected such p from the set of all rational primes with probability about 1/2.

Remark 2: Note that, in Step 5 of the key generation stage, for any subset $\{p_{i_1}, p_{i_2}, \ldots, p_{i_k}\}$ from $\{p_1, p_2, \ldots, p_n\}$, $\prod_{j=1}^{k} \mathcal{N}(p_{i_j}) = \mathcal{N}(\prod_{j=1}^{k} p_{i_j}) < \frac{p^2}{4}$, (or $\frac{(p-1)^2 D}{4(1+D)}$), so $\prod_{j=1}^{k} p_{i_j} \in R(\mathfrak{p})$ by Proposition 3. That is, there exist integers $a_1, a_2 \in \mathbb{Z}$ $(-p/2 < a_1, a_2 < p/2)$ such that $u = a_1 + a_2\omega_2$ in Step 3(a) of the Decryption. The typical selection of $p_1, \ldots, p_n$ presented in Section 3.4 may be restricted, in fact, we take $p_1, \ldots, p_n$ from the rational integers, but the selection introduced above is more general than the typical one. That is, we can take p_i's from $\mathbb{Z}$ as well as $\mathcal{O}_K$ by using such a characterization with the norm in the imaginary quadratic field case.