J. Cryptology (2000) 13: 263–272
DOI: 10.1007/s001459910010

Journal of
CRYPTOLOGY

A New Public-Key Cryptosystem over a Quadratic Order with Quadratic Decryption Time

Sachar Paulus
Technische Universität Darmstadt,
Alexanderstrasse 10, D-64283 Darmstadt, Germany

Tsuyoshi Takagi
NTT Software Laboratories,
3-9-11 Midori-cho Musashino-shi,
Tokyo 180, Japan

Communicated by J. Buchmann

Received 29 June 1998 and revised 15 November 1998

Abstract. We present a new cryptosystem based on ideal arithmetic in quadratic orders. The method of our trapdoor is different from the Diffie–Hellman key distribution scheme or the RSA cryptosystem. The plaintext $\mathfrak{m}$ is encrypted by $\mathfrak{m}\mathfrak{p}^r$, where $\mathfrak{p}$ is a fixed element and r is a random integer, so our proposed cryptosystem is a probabilistic encryption scheme and has the homomorphy property. The most prominent property of our cryptosystem is the cost of the decryption, which is of quadratic bit complexity in the length of the public key. Our implementation shows that it is comparably as fast as the encryption time of the RSA cryptosystem with $e = 2^{16} + 1$. The security of our cryptosystem is closely related to factoring the discriminant of a quadratic order. When we choose appropriate sizes of the parameters, the currently known fast algorithms, for example, the elliptic curve method, the number field sieve, the Hafner–McCurley algorithm, are not applicable. We also discuss that the chosen ciphertext attack is not applicable to our cryptosystem.

Key words. Public-key cryptosystem, Fast decryption, Quadratic order, Factoring algorithm, Chosen ciphertext attack.

1. Overview

Plenty of public-key cryptosystems have been proposed, and the Diffie–Hellman key distribution scheme or the RSA cryptosystem are mostly used throughout the world [9], [22]. Typically, these public-key cryptosystems involve a modular exponentiation with a large number, which is of cubic bit complexity in the bit length of the public key and its computation is relatively slow. On the other side, for the sake of high security the secret keys are stored on a smart card and the decryption computation is also

carried out over the smart card. So a cryptosystem with fast decryption is desired. To our knowledge, there exists no practical public key cryptosystem which has quadratic decryption time. In this paper we present a new cryptosystem with fast decryption time. The decryption is of quadratic bit complexity; it involves an extended Euclidean algorithm computation, an ideal reduction and a few basic operations like multiplication and division with remainder of numbers. By the experiment of our implementation, our cryptosystem is comparably as fast as the encryption time of the RSA cryptosystem with $e = 2^{16} + 1$.

Our cryptosystem is constructed over an imaginary quadratic field. Buchmann and Williams proposed the first algorithm which achieves the Diffie–Hellman key distribution scheme using the class group in an imaginary quadratic field [5]. Later, Hafner and McCurley discovered the subexponential algorithm against the discrete logarithm problem of the class group [13]. Since then cryptosystems over class groups have not gained much attention in practice. Recently, Hühnlein et al. proposed an ElGamal-type public-key cryptosystem with a faster decryption process in class groups of imaginary quadratic fields [14]. Here we call it the HJPT cryptosystem. Denote by $Cl(\Delta_q)$ and $Cl(\Delta_1)$ the class group of the nonmaximal order and that of the maximal order, respectively. The technique used in the HJPT cryptosystem is to "switch" the ideals between $Cl(\Delta_q)$ and $Cl(\Delta_1)$. Note that the arithmetic of the switching is fast, i.e., has quadratic complexity in the bit length of the public key. Nevertheless, the HJPT cryptosystem has cubic decryption time because it is an ElGamal-type public-key cryptosystem and involves an exponentiation step. In our case, we encrypt the plaintext $\mathfrak{m}$ by $E(\mathfrak{m}, r) = \mathfrak{m}\mathfrak{p}^r$, where $\mathfrak{p}$ is an element in the kernel of the map $Cl(\Delta_q) \to Cl(\Delta_1)$ and r is a random integer. By this encryption, the decryption process only involves the switching arithmetic, so the decryption has quadratic complexity in the bit length of the public key. The encryption process $E(\mathfrak{m}, r) = \mathfrak{m}\mathfrak{p}^r$ induces that our cryptosystem uses a probabilistic encryption and the homomorphy property.

The security of our cryptosystem is based upon a new number-theoretic problem over quadratic orders which is closely related to factoring the discriminant $\Delta_q = -pq^2$. When we choose appropriate sizes of the parameters, the currently known fast algorithms like the elliptic curve method [15], the number field sieve [16], and the Hafner–McCurley algorithm [13] are not applicable. We also discuss the chosen ciphertext attack. In our cryptosystem, the surjective one way map $Cl(\Delta_q) \to Cl(\Delta_1)$ plays an important role. Two public key cryptosystems which use such a surjective map are known: Shamir's *RSA for paranoids* which uses $(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ $(n = pq)$ [25] and the Okamoto–Uchiyama cryptosystem which uses $(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^+$ $(n = p^2q)$ [20]. The chosen ciphertext attack is applicable to both public key cryptosystems, and the attacker can easily factor the public modulus n (see, for example, [12]). However, the chosen ciphertext attack is not applicable to our cryptosystem.

The paper is organized as follows: we first recall the basic notions of class groups of quadratic orders and describe how to "switch" from the nonmaximal order to the maximal order and vice versa. We then present the new cryptosystem and analyze its security. Finally, we give some timings comparing our new cryptosystem with RSA.

2. Quadratic Orders

There are plenty of cryptographic primitives using quadratic fields and several public-key cryptosystems are proposed [6]. We briefly explain the class group of a quadratic order. A more complete treatment may be found in [8].

Let $\Delta \in \mathbb{Z}$ not a square such that $\Delta \equiv 0, 1 \pmod 4$. We call Δ a (*quadratic*) *discriminant*. Δ is called a *fundamental* discriminant if $\Delta \equiv 1 \pmod 4$ and is square-free, or $\Delta/4 \equiv 2, 3 \pmod 4$ and is square-free. Every discriminant Δ can be represented by $\Delta_1 f^2$, where Δ_1 is a fundamental discriminant and f is an integer, and we denote $\Delta_f = \Delta_1 f^2$. We consider only negative discriminants in this paper. Let $\sqrt{\Delta_f} = i\sqrt{|\Delta_f|}$ be the square root of Δ_f on the upper half-plane. Then we call $\mathcal{O}_{\Delta_f} = \mathbb{Z} + ((\Delta_f + \sqrt{\Delta_f})/2)\mathbb{Z}$ the *quadratic order* of discriminant Δ_f. It is an integral domain. If Δ_f is not a fundamental discriminant, then $\mathcal{O}_{\Delta_f} \subset \mathcal{O}_{\Delta_1}$ and $\mathcal{O}_{\Delta_f}$ has finite index f in $\mathcal{O}_{\Delta_1}$. Moreover, we have $\mathcal{O}_{\Delta_f} = \mathbb{Z} + f\mathcal{O}_{\Delta_1}$. The order $\mathcal{O}_{\Delta_f}$ is called the *nonmaximal order* with *conductor* f, and the order $\mathcal{O}_{\Delta_1}$ is called the *maximal order*. Every element $\alpha \in \mathcal{O}_{\Delta_f}$ is represented by $\alpha = (x+y\sqrt{\Delta_f})/2$, $x, y \in \mathbb{Z}$. For $\alpha = (x+y\sqrt{\Delta_f})/2$, we denote by $\alpha' = (x-y\sqrt{\Delta_f})/2$ its (complex) conjugate. The *norm* of α is defined as $N(\alpha) = \alpha\alpha' = (x^2 - y^2\Delta_f)/4$. A subset $\mathfrak{a}$ of $\mathcal{O}_{\Delta_f}$ is an (integral) ideal of $\mathcal{O}_{\Delta_f}$ if $\alpha + \beta \in \mathfrak{a}$ whenever $\alpha, \beta \in \mathfrak{a}$, and $\alpha(\Delta_f + \sqrt{\Delta_f})/2 \in \mathfrak{a}$ whenever $\alpha \in \mathfrak{a}$. Every ideal $\mathfrak{a}$ of $\mathcal{O}_{\Delta_f}$ is given by

$$\mathfrak{a} = m\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta_f}}{2}\mathbb{Z}\right), \tag{1}$$

where $m \in \mathbb{Z}$, $a \in \mathbb{Z}_{>0}$, and $b \in \mathbb{Z}$ such that $b^2 \equiv \Delta_f \pmod{4a}$. This expression is unique if we choose $-a < b \leq a$. Then (m, a, b) is called the *standard representation* of $\mathfrak{a}$. The *norm* of an ideal $\mathfrak{a}$ is defined by $N(\mathfrak{a}) = am$. $\mathfrak{a}$ is said to be *primitive* if $m = 1$. In that case, we represent $\mathfrak{a}$ by (a, b). For two given ideals $\mathfrak{a}, \mathfrak{b}$, we can define their product $\mathfrak{a}\mathfrak{b}$ (see, for example, [5]). The computation of a representation of $\mathfrak{a}\mathfrak{b}$ needs $O((\log(\max\{N(\mathfrak{a}), N(\mathfrak{b})\}))^2)$ bit operations.

We describe the class group of $\mathcal{O}_{\Delta_f}$. An ideal $\mathfrak{a}$ is called *prime* to f if $\mathrm{GCD}(N(\mathfrak{a}), f) = 1$ holds. The ideals of $\mathcal{O}_{\Delta_f}$ prime to f form an Abelian group; denote it by $\mathcal{I}_{\Delta_f}(f)$. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called *equivalent* if there is an $\alpha \in \mathcal{O}_{\Delta_f}$ such that $\mathfrak{a} = \alpha\mathfrak{b}$. Denote this equivalence relation by $\mathfrak{a} \sim \mathfrak{b}$. For an element $\gamma \in \mathcal{O}_{\Delta_f}$ the ideal $\gamma\mathcal{O}_{\Delta_f}$ is called a *principal* ideal. The principal ideals $\mathcal{P}_{\Delta_f}(f)$ which are prime to f form a subgroup of $\mathcal{I}_{\Delta_f}(f)$. The quotient group $\mathcal{I}_{\Delta_f}(f)/\mathcal{P}_{\Delta_f}(f)$ is called the *class group* of $\mathcal{O}_{\Delta_f}$; denote it by $Cl(\Delta_f)$. The order of this group is denoted by $h(\Delta_f)$. For a primitive ideal $\mathfrak{a}$ in $\mathcal{I}_{\Delta_f}(f)$, we say that $\mathfrak{a} = (a, b)$ is *reduced* if $|b| \leq a \leq c = (b^2 - \Delta_f)/4a$ and additionally $b \geq 0$ if $a = c$ or $a = |b|$. There is only one reduced ideal in every equivalence class. Denote by $Red_{\Delta_f}(\mathfrak{a})$ the reduced ideal equivalent to $\mathfrak{a} \in \mathcal{I}_{\Delta_f}(f)$. An algorithm to compute $Red_{\Delta_f}(\mathfrak{a})$ from $\mathfrak{a}$ is described in [5] and requires $O((\log(N(\mathfrak{a})))^2)$ bit operations. We identify each class of the class group with the unique reduced ideal. It is easy to verify that $N(\mathfrak{a}) < \sqrt{|\Delta_f|/3}$ holds for every reduced ideal $\mathfrak{a} \in \mathcal{I}_{\Delta_f}(f)$. Conversely, a primitive ideal $\mathfrak{a} \in \mathcal{I}_{\Delta_f}(f)$ with small norm such that $N(\mathfrak{a}) < \sqrt{|\Delta_f|/4}$ is always a reduced ideal. It turns out that we can compute the representation of the product of two classes of the class group in $O((\log\sqrt{|\Delta_f|})^2)$ bit operations. See [2].

2.1. *The Map $Cl(\Delta_q) \to Cl(\Delta_1)$*

In [8] the relationship between ideals in the maximal order $\mathcal{O}_{\Delta_1}$ and in the nonmaximal order $\mathcal{O}_{\Delta_f}$ is investigated. If $\mathfrak{a}$ is an ideal in $\mathcal{I}_{\Delta_f}(f)$, then $\mathfrak{A} = \mathfrak{a}\mathcal{O}_{\Delta_1}$ is an ideal in $\mathcal{I}_{\Delta_1}(f)$ and $N(\mathfrak{a}) = N(\mathfrak{A})$. Similarly, if $\mathfrak{A}$ is an ideal in $\mathcal{I}_{\Delta_1}(f)$, then $\mathfrak{a} = \mathfrak{A} \cap \mathcal{O}_{\Delta_f}$ is an ideal in $\mathcal{I}_{\Delta_f}(f)$ and $N(\mathfrak{A}) = N(\mathfrak{a})$. The map $\varphi : \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{\Delta_1}$ induces an isomorphism $\mathcal{I}_{\Delta_f}(f) \tilde{\to} \mathcal{I}_{\Delta_1}(f)$. The inverse of this map is $\varphi^{-1} : \mathfrak{A} \mapsto \mathfrak{A} \cap \mathcal{O}_{\Delta_f}$. Let $f = q$ be a prime and let $\sqrt{|\Delta_1|/3} < q$. Then all the reduced ideals in $Cl(\Delta_1)$ are prime to the conductor q [14]. Thus we can consider the following map based on φ:

$$\begin{aligned} \varphi_q : \quad Cl(\Delta_q) &\longrightarrow Cl(\Delta_1), \\ \mathfrak{a} &\longmapsto Red_{\Delta_1}(\mathfrak{a}\mathcal{O}_{\Delta_1}), \end{aligned}$$

where we identify a class of both class groups with the unique reduced ideal in that class. (Note that if $q > \sqrt{|\Delta_1|/3}$ we can also define this map; we possibly have to compute an ideal equivalent to $\mathfrak{a}$ which is prime to q. See [14].) A practical algorithm to compute φ_q is as follows:

Algorithm 1 (GoToMaxOrder)

Input: A reduced ideal $\mathfrak{a} = (a, b) \in Cl(\Delta_q)$, the discriminant Δ_q, the fundamental discriminant Δ_1, and the conductor q.
Output: A reduced ideal $\mathfrak{A} = \varphi_q(\mathfrak{a}) = (A, B)$.

1. $A \leftarrow a$
2. $b_{\mathcal{O}} \leftarrow \Delta_q \bmod 2$
3. Solve $1 = \mu q + \lambda a$ for $\mu, \lambda \in \mathbb{Z}$ using the extended Euclidean algorithm
4. $B \leftarrow b\mu + a b_{\mathcal{O}} \lambda \bmod 2a$
5. $(A, B) \leftarrow Red_{\Delta_1}(A, B)$
6. RETURN (A, B)

Note that the map GoToMaxOrder is different from the map described in [14]. Every step of this algorithm requires $O((\log \sqrt{|\Delta_q|})^2)$ bit operations, thus the complexity of this algorithm is quadratic.

We discuss the "inverse" map φ_q^{-1}. The map $\varphi_q : Cl(\Delta_q) \to Cl(\Delta_1)$ is surjective and we have $h(\Delta_q) = h(\Delta_1)(q - (\Delta_1/q))$, where (Δ_1/q) is the Kronecker-symbol (see, for example, [8]). Denote by $\mathrm{Ker}(\varphi_q)$ the kernel of the map $\varphi_q : Cl(\Delta_q) \to Cl(\Delta_1)$ which is a cyclic subgroup of $Cl(\Delta_q)$ with order $q - (\Delta_1/q)$. So there is a $(q - (\Delta_1/q))$-fold ambiguity for the inverse of the map φ_q. We distinguish a unique reduced ideal from these preimages using the size of the norm of an ideal. The norm of any reduced ideal in $Cl(\Delta_1)$ is smaller than $\sqrt{|\Delta_1|/3}$. By our assumption $\sqrt{|\Delta_1|/3} < q$ all ideals in $Cl(\Delta_1)$ are prime to the conductor q. Therefore, for a reduced ideal $\mathfrak{A}$ in $Cl(\Delta_1)$, $\mathfrak{a} = \varphi^{-1}(\mathfrak{A}) = \mathfrak{A} \cap \mathcal{O}_{\Delta_q}$ is a primitive ideal in $\mathcal{I}_{\Delta_q}(q)$, and $N(\mathfrak{A}) = N(\mathfrak{a})$. If the primitive ideal $\mathfrak{a}$ in $\mathcal{I}_{\Delta_q}(q)$ satisfies $N(\mathfrak{a}) < \sqrt{|\Delta_1|/4}$, then both $\mathfrak{a}$ and $\mathfrak{A}$ are reduced ideals. Consequently, if we restrict ourselves to ideals $\mathfrak{a}$ in $Cl(\Delta_q)$ such that $N(\mathfrak{a}) < \sqrt{|\Delta_1|/4}$, then $\varphi_q(\mathfrak{a}) \cap \mathcal{O}_{\Delta_q}$ is reduced (in $\mathcal{I}_{\Delta_q}(q)$) and so we can compute a distinguished inverse of the map φ_q, namely, $\mathfrak{a}$. Note that the cardinality of this set is smaller than that of $Cl(\Delta_1)$. We denote

by φ_q^{-1} this restricted inverse map and the practical algorithm to compute the map φ_q^{-1} is as follows:

Algorithm 2 (Inverse)

Input: A reduced ideal $\mathfrak{A} = (A, B) \in Cl(\Delta_1)$ such that $N(\mathfrak{A}) < \sqrt{|\Delta_1|/4}$, the conductor q.
Output: A reduced ideal $\mathfrak{a} \in Cl(\Delta_q)$ such that $\varphi_q^{-1}(\mathfrak{A}) = \mathfrak{a} = (a, b)$.

1. $a \leftarrow A$
2. $b \leftarrow Bq \bmod 2a$
3. RETURN (a, b)

This algorithm obviously requires only $O((\log(\sqrt{|\Delta_1|}))^2)$ bit operations.

3. The New Cryptosystem

Generate two random primes $p, q > 4$ such that $p \equiv 3 \pmod 4$ and let $\Delta_1 = -p$. Let $Cl(\Delta_1)$ be the class group of the maximal order with discriminant Δ_1 and let $Cl(\Delta_q)$ be the class group of the nonmaximal order with conductor q. Δ_q will be public, whilst its factorization into Δ_1 and q will be kept private. The discriminant Δ_1 and the conductor q are large primes to prevent breaking the cryptosystem by factoring Δ_q.

In the key generation, we choose an ideal $\mathfrak{p}$ from the kernel $\mathrm{Ker}(\varphi_q)$ and make $\mathfrak{p}$ public. The message ideal $\mathfrak{m}$ is a reduced ideal in $Cl(\Delta_q)$ with norm smaller than $\lfloor\sqrt{|\Delta_1|/4}\rfloor$. The encryption is carried over the class group $Cl(\Delta_q)$ by computing $Red_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$, where r is a random integer smaller than $q - (\Delta_1/q)$. Then, by the knowledge of the conductor, we can go to the maximal order and the image of the message ideal $\varphi_q(\mathfrak{m})$ in the maximal order is revealed, since $\varphi_q(\mathfrak{m}\mathfrak{p}^r) = \varphi_q(\mathfrak{m})\varphi_q(\mathfrak{p}^r) = \varphi_q(\mathfrak{m})\mathcal{O}_{\Delta_1} = \varphi_q(\mathfrak{m})$. We can recover the message by computing the unique preimage of $\varphi_q(\mathfrak{m})$, namely, $\mathfrak{m} = \varphi_q^{-1}(\varphi(m))$.

1. **Key generation:** Generate two random primes $p, q > 4$ with $p \equiv 3 \pmod 4$ and $\sqrt{p/3} < q$. Let $\Delta_1 = -p$ and $\Delta_q = \Delta_1 q^2$. Let k and l be the bit lengths of $\lfloor\sqrt{|\Delta_1|/4}\rfloor$ and $q - (\Delta_1/q)$, respectively. Choose an ideal $\mathfrak{p}$ in $Cl(\Delta_q)$, where
$$\varphi_q(\mathfrak{p}) \text{ is a principal ideal in } \mathcal{O}_{\Delta_1}. \tag{2}$$
Then $(\mathfrak{p}, \Delta_q, k, l)$ are the system parameters, and Δ_1, q are the secret keys.
2. **Encryption:** Let $\mathfrak{m}$ be the plaintext, where $\mathfrak{m}$ is a reduced ideal in $Cl(\Delta_q)$ with $\log_2 N(\mathfrak{m}) < k$. Pick up a random $l - 1$ bit integer and encrypt the plaintext as follows using binary exponentiation techniques:
$$\mathfrak{c} = Red_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r). \tag{3}$$
Then $\mathfrak{c}$ is the ciphertext.
3. **Decryption:** Using the secret keys Δ_1, q, we compute $\mathfrak{K} = \mathsf{GoToMaxOrder}(\mathfrak{c})$. The plaintext $\mathfrak{m}$ can be recovered by computing $\mathfrak{m} = \mathsf{Inverse}(\mathfrak{K})$.

The embedding of a number into a message ideal may be simply done as follows: let x be a message and let t be a random number of length $k - 2 - \lfloor\log_2 x\rfloor$. Denote by $x.t$

the concatenation of x and t as bitstrings. We determine the smallest prime l larger than $x.t$ with $(\Delta_q/l) = 1$. It follows that $\log_2 l < k - 1$. This can be done effectively using a few trials of a primality test and Jacobi symbol computations. Then, compute b such that $\Delta_q \equiv b^2 \bmod 4l$, $-l < b \leq l$. This can also be done effectively using the RESSOL algorithm of Shanks [26]. Then $\mathfrak{a} = (l, b)$ is a reduced ideal with $\log_2 N(\mathfrak{a}) < k$.

The key generation simply works as follows: choose a number $\alpha \in \mathcal{O}_{\Delta_1}$ with norm less than $\sqrt{|\Delta_q|/4}$, compute the standard representation of the ideal $\alpha\mathcal{O}_{\Delta_1}$, and compute $\mathfrak{p} = \varphi^{-1}(\alpha\mathcal{O}_{\Delta_1})$. This is explained in [14]. Then $\mathfrak{p} \in \ker\varphi_q$. The encryption takes $O((\log\sqrt{|\Delta_q|})^3)$ bit operations because of the binary exponentiation. The decryption involves two algorithms of quadratic complexity, so it requires only $O((\log\sqrt{|\Delta_q|})^2)$ bit operations.

4. Security Considerations

The security of our cryptosystem depends on the difficulty of factoring the discriminant Δ_q. If the discriminant Δ_q can be factored, our proposed cryptosystem is completely broken. First, we consider the size of the secret parameters Δ_1 and q to prevent breaking the cryptosystem by factoring Δ_q. On the other hand, an attacker may somehow compute the image $\varphi(\mathfrak{a})$ in the maximal order $\mathcal{O}_{\Delta_1}$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_{\Delta_q}$. We prove that to compute the map $\varphi(\mathfrak{a})$ is as intractable as factoring Δ_q. In our cryptosystem, we make public an ideal $\mathfrak{p}$ in $\mathrm{Ker}(\varphi_q)$. We discuss that according to current knowledge the knowledge of such an ideal does not bring any advantage for factoring the discriminant. Finally, we argue that a chosen ciphertext attack as presented in [12] against Shamir's RSA variant [25] will not give us substantially more knowledge than was previously known.

4.1. *The Size of the Secret Parameters* Δ_1, q

We discuss the size of the secret parameters $\Delta_1 = -p$ and q which prevents attacks by the known factoring algorithms. Let $L_N[s, c] = \exp((c + o(1))\log^s(N)\log\log^{1-s}(N))$. The number field sieve [16] and the elliptic curve method [15] are the different types of factoring algorithms which have to be taken care of; other factoring algorithms are more or less slower [18], [23]. The number field sieve is the fastest factoring algorithm, and the running time depends on the total bit length of the composite number $|\Delta_q|$; it is of the order of $L_{|\Delta_q|}[\frac{1}{3}, (\frac{64}{9})^{1/3}]$. Currently the fastest implementation for the number field sieve factored a 130-digit ($\approx$ 431-bit) RSA modulus [7]. If we choose Δ_q to be larger than 768 bits, the number field sieve becomes infeasible. On the other hand, the elliptic curve method depends on the size of the primes p or q and the expected running time is $L_r[\frac{1}{2}, 2^{1/2}]$, where r is p or q. The fastest implementation for the elliptic curve method found a 48-digit ($\approx$ 159-bit) prime factor [10]. If we choose p and q to be larger than 256 bits, the elliptic curve method becomes infeasible. Therefore, the 768-bit discriminant Δ_q with 256-bit p, q is secure for cryptographic purposes.

We wonder if there exists a special algorithm for factoring a composite number with a squared prime factor. To our knowledge, the only algorithm for this problem presented is by Peralta and Okamoto [21]. They improve the elliptic curve method by a constant factor by considering the distribution of the Jacobi symbol. For example, for finding

the 40-digit ($\approx$ 133-bit) prime factor, the algorithm is 25 times faster than the original elliptic curve method. Its improvement is negligible and is not a real threat.

4.2. *Security of* φ

Only the person who knows the conductor q can compute the map φ_q and then recover any message ideal. The map φ_q consists of $\varphi_q = Red_{\Delta_1} \circ \varphi$. If attackers somehow can compute the ideal $\varphi(\mathfrak{a})$ in the maximal order which is the image of an ideal $\mathfrak{a}$ in $Cl(\Delta_q)$, then the message ideal $\mathfrak{m}$ may be recovered. Here, we can prove that the discriminant Δ_q can be factored using few iterations of any algorithm which computes the image of φ.

Theorem 1. *Assume that there exists an algorithm* $\mathbf{AL}_\varphi$ *which computes for the primitive ideal* $\mathfrak{a} = (a_1, a_2) \in \mathcal{I}_{\Delta_q}(q)$ *a primitive ideal* $\mathfrak{A} = (A_1, A_2) \in \mathcal{I}_{\Delta_1}(q)$ *such that* $\mathfrak{A} = \varphi(\mathfrak{a})$ *without knowing the conductor* q. *By using the algorithm* $\mathbf{AL}_\varphi$ *as an oracle, the discriminant* $\Delta_q = \Delta q^2$ *can be factored in random polynomial time.*

Proof. Let $\mathfrak{a} = (a, b)$ be a primitive ideal in $\mathcal{I}_{\Delta_q}(q)$. By using the algorithm $\mathbf{AL}_\varphi$, we can compute $\mathfrak{A} = (A, B)$ such that $\mathfrak{A} = \varphi(\mathfrak{a})$. The relation between the ideals $\mathfrak{a}$ and $\mathfrak{A}$ is as follows:

$$a = A, \qquad B \equiv bq^{-1} \pmod{a}. \tag{4}$$

Therefore, we can compute $q \equiv bB^{-1} \pmod{a}$ because $(B, a) = (b, a) = 1$. We apply this algorithm for several prime ideals $\mathfrak{p}_i = (p_i, b_{p_i})$, where p_i is prime with $(p_i/\Delta_q) = 1$, which require random polynomial time in generating them. After polynomially many iterations in $\log_2 \Delta_q$, we can recover the conductor q using the Chinese Remainder Theorem. It is easy to check the right q by computing the greatest common divisor with Δ_q. □

This theorem means that nobody can "switch" the primitive ideal (a, b) to the maximal order without the knowledge of the conductor q.

4.3. *Knowledge of* $\mathfrak{p}$

Let $\mathfrak{p}$ be the public key which is the element in $\mathrm{Ker}(\varphi_q)$. We argue that the knowledge of $\mathfrak{p}$ does not substantially help to factor Δ_q using currently known fast algorithms. For simplicity, we assume $\mathfrak{p}$ is the generator of the group $\mathrm{Ker}(\varphi_q)$, so the order of $\mathfrak{p}$ is $q - (q/\Delta_1)$. A nontrivial ambiguous ideal is an ideal $\mathfrak{f}$ in $Cl(\Delta_q)$ such that $\mathfrak{f}^2 \sim 1$ and $\mathfrak{f} \not\sim 1$. If a nontrivial ambiguous ideal in the order $\mathcal{O}_{\Delta_q}$ is known, we can factor the discriminant Δ_q [24]. For the discriminant Δ_q of our cryptosystem, there is only one nontrivial ambiguous ideal in $Cl(\Delta_q)$. Moreover, the nontrivial ambiguous ideal lies in the group $\mathrm{Ker}(\varphi_q)$, so the probability that $\mathfrak{p}^r$ for a random r will be a nontrivial ambiguous ideal is negligible. It is unknown whether other ideals in $\mathrm{Ker}(\varphi_q)$ except the ambiguous ideals can be used for factoring the discriminant Δ_q.

In our cryptosystem, we publish the ideal $\mathfrak{p}$. A possible attack to find a nontrivial ambiguous ideal for a given $\mathfrak{p}$ is to compute the order of $\mathfrak{p}$ in the group $Cl(\Delta_q)$. The fastest algorithm to compute the order of $\mathfrak{p}$ in the group $Cl(\Delta_q)$ is the Hafner–McCurley

algorithm [13]. Its running time is $L_{|\Delta_q|}[\frac{1}{2}, 2^{1/2}]$ which is much slower than factoring Δ_q. This shows that with the currently known algorithms, knowledge of $\mathfrak{p}$ does not with high probability help in factoring Δ_q. The same reasoning applies for polynomially many elements of $\mathrm{Ker}(\varphi_q)$.

4.4. *Chosen Ciphertext Attack*

Let G_1, G_2 be finite abelian groups and consider a surjective homomorphism $\varphi : G_1 \to G_2$. If two elements g, h in G_1 satisfy $\varphi(g) = \varphi(h)$, then we assume them *to be in the same coset*. Our cryptosystem is constructed using the surjective homomorphism $\varphi_q : Cl(\Delta_q) \to Cl(\Delta_1)$. The message ideal $\mathfrak{m}$ is encrypted by $\mathfrak{c} = Red_{\Delta_q}(\mathfrak{m}\mathfrak{p}^r)$. Then the ciphertext $\mathfrak{c}$ "represents" all elements of the coset of $\mathfrak{m}$ in the group $Cl(\Delta_q)$.

Similarly, Shamir proposed an RSA type public key cryptosystem using the homomorphism $\varphi_S : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$, where $n = pq$ and p, q are primes [25]. In the key generation, e, d are generated by the relation $ed \equiv 1 \pmod{p-1}$. The message M must be smaller than p. For the encryption we compute $C \equiv M^e \pmod{n}$, and the message can be recovered by $M \equiv C^d \pmod{p}$. For an element $a \in (\mathbb{Z}/n\mathbb{Z})^*$, all elements of the coset of a for the map φ_S are represented by $\{a, a+p, a+2p, \ldots, a+(q-1)p\}$. Therefore, if we know two elements a_1, a_2 in the same coset, we can factor the modulus n by computing $\mathrm{GCD}(a_1 - a_2, n) = p$. This is equivalent to the fact that n can be factored if we know an element in the kernel of φ_S. Using this Gilbert et al. proposed the following attack against this cryptosystem [12]. Let M' be a message larger than p, and let C be the ciphertext corresponding to M'. If an attacker can know the plaintext corresponding to C, say M, then the modulus n can be factored by computing $\mathrm{GCD}(M - M', n)$. We call this attack the *chosen ciphertext attack*.[1] Note that this chosen ciphertext can be achieved because $\mathbb{Z}/n\mathbb{Z}$ is not only a group but also a ring.

Consider the chosen ciphertext attack against our proposed cryptosystem. Let $\mathfrak{m}'$ be a message ideal such that $N(\mathfrak{m}') > \sqrt{|\Delta_1|/3}$. If $\mathfrak{m}$ is the regular message ideal which is a reduced ideal with norm smaller than $\sqrt{|\Delta_1|/4}$ and in the same coset of $\mathfrak{m}'$, then we have $\mathfrak{m} \sim \mathfrak{m}'\mathfrak{p}^s$ for some integer $s \geq 0$. This yields the knowledge of some other $\mathfrak{p}' \in \mathrm{Ker}(\varphi_q)$. As shown above, no algorithm is known to compute the factorization of Δ_q when polynomially many elements of the kernel are known. Next, we discuss the case where the chosen ciphertext attack is applied several times. Denote by $\mathbf{AL}_C$ the oracle which, given as input an ideal $\mathfrak{m}'$ in $\mathcal{O}_{\Delta_q}$, answers with the reduced ideal $\mathfrak{m}$ with norm smaller than $\sqrt{|\Delta_1|/4}$ such that $\varphi_q(\mathfrak{m}) = \varphi(\mathfrak{m}')$ in $Cl(\Delta_1)$. By the answer of this oracle $\mathbf{AL}_C$, we can to some extent deduce information about Δ_1. Indeed, we have the following relations:

$$\begin{aligned} \mathbf{AL}_C(\mathfrak{m}') \neq \mathfrak{m} \quad &\Rightarrow \quad N(\mathfrak{m}') > \sqrt{|\Delta_1|/4}, \\ \mathbf{AL}_C(\mathfrak{m}') = \mathfrak{m} \quad &\Rightarrow \quad N(\mathfrak{m}') < \sqrt{|\Delta_1|/3}. \end{aligned}$$

Note that if $\sqrt{|\Delta_1|/4} < N(\mathfrak{m}') < \sqrt{|\Delta_1|/3}$, the oracle $\mathbf{AL}_C$ may answer the same ideal or a different ideal, depending on $\varphi(\mathfrak{m}')$ being a reduced ideal or not. Since this range

[1] Okamoto and Uchiyama proposed the public-key cryptosystem using the homomorphism $\varphi_{OU} : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^+$, where $n = p^2q$ and p, q are primes [20]. This chosen ciphertext attack is also applicable against the Okamoto–Uchiyama cryptosystem.

Table 1. Average timings for the new cryptosystem compared with RSA ($e = 2^{16}+1$) over 100 randomly chosen pairs of primes of the specified size on a SPARC station 4 (110 MHz) using the LiDIA library

$\log_2(n)$	768	1024	1536	2048
RSA encryption	6 ms	10 ms	19 ms	31 ms
RSA classical decryption	470 ms	1,032 ms	3,045 ms	7,006 ms
New CS precomputation for $p \approx q \approx n^{1/3}$	3,759 ms	7,650 ms	21,682 ms	36,166 ms
New CS encryption for $p \approx q \approx n^{1/3}$	3 ms	4 ms	8 ms	12 ms
New CS decryption for $p \approx q \approx n^{1/3}$	8 ms	13 ms	22 ms	30 ms
New CS precomputation for $p \approx n^{1/4}$	—	8,766 ms	24,673 ms	36,276 ms
New CS encryption for $p \approx n^{1/4}$	—	4 ms	6 ms	10 ms
New CS decryption for $p \approx n^{1/4}$	—	12 ms	22 ms	32 ms

has size about $0.07735\sqrt{|\Delta_1|}$, it would take an exponential number (in $\log_2 \sqrt{|\Delta_1|}$) of queries to $\mathbf{AL}_C$ to detect a good approximation of either $\sqrt{|\Delta_1|/4}$ or $\sqrt{|\Delta_1|/3}$. Therefore, the chosen ciphertext attack is not applicable to our proposed cryptosystem.

5. Practicality

The prominent property of the proposed cryptosystem is the running time of the decryption. Most prominent cryptosystems require decryption time $O((\log_2 n)^3)$, where n is the size of the public key. The total running time of the decryption process of our cryptosystem is $O((\log_2 \Delta_q)^2)$ bit operations. In order to demonstrate the improved efficiency of our decryption, we implemented our scheme using the LiDIA library [3]. It should be emphasized here that our implementation was not optimized for cryptographic purposes—it is only intended to provide a comparison between decrypting in the nonmaximal order and using our trapdoor decryption. The results are shown in Table 1.

Observe that we separated the fast exponentiation step of the encryption as a "precomputation" stage. Indeed, if we can securely store the values $\mathfrak{p}^r$, then the actual encryption can be effected very rapidly, since it requires only one ideal multiplication and one ideal reduction. Of course, one can use one of the well-known fixed-base exponentiation techniques completely analogously as for ElGamal-type protocols as mentioned, e.g., in Section 14.6.3 of [18].

It should be mentioned that the size of a message for our cryptosystem is smaller than the size of a message for the RSA encryption (e.g., 256 bit versus 768 bit, or 341 bit versus 1024 bit). In connection with the very fast decryption time, an excellent purpose for our cryptosystem could be (symmetric) key distribution. In that setting, the short message length is not a real drawback. On the other hand, the message length is longer than for ElGamal encryption on "comparably" secure elliptic curves (e.g., 341 bit versus 180 bit).

Acknowledgments

We thank Johannes Buchmann for several helpful comments.

References

[1] L. M. Adleman and K. S. McCurley; Open problems in number theoretic complexity, II *Proceedings of ANTS-I*, LNCS 877, Springer-Verlag, Berlin (1994), pp. 291–322.

[2] I. Biehl and J. Buchmann; An analysis of the reduction algorithms for binary quadratic forms, Technical Report No. TI-26/97, Technische Universität Darmstadt, Darmstadt (1997).

[3] I. Biehl, J. Buchmann, and T. Papanikolaou; *LiDIA—A Library for Computational Number Theory*, The LiDIA Group, Universität des Saarlandes, Saarbrücken (1995).

[4] J. Buchmann, S. Düllmann, and H. C. Williams; On the complexity and efficiency of a new key exchange system, *Advances in Cryptology – EUROCRYPT* '89, LNCS 434, Springer-Verlag, Berlin (1990), pp. 597–616.

[5] J. Buchmann and H. C. Williams; A key-exchange system based on imaginary quadratic fields, *Journal of Cryptology*, **1** (1988), 107–118.

[6] J. Buchmann and H. C. Williams; *Quadratic fields and cryptography*, London Mathematical Society Lecture Note Series 154, Cambridge University Press, Cambridge (1990), pp. 9–26.

[7] J. Cowie, B. Dodson, R. Elkenbracht-Huizing, A. K. Lenstra, P. L. Montgomery, and J. Zayer; A world wide number field sieve factoring record: on to 512 bits, *Advances in Cryptology – ASIACRYPT* '96, LNCS 1163, Springer-Verlag, Berlin (1996), pp. 382–394.

[8] D. A. Cox; *Primes of the Form* $x^2 + ny^2$, Wiley, New York (1989).

[9] W. Diffie and M. Hellman; New directions in cryptography, *IEEE Transactions on Information Theory*, **22** (1976), 472–492.

[10] ECMNET Project; `http://www.loria.fr/~zimmerma/records/ecmnet.html`.

[11] T. ElGamal; A public key cryptosystem and a signature scheme based on discrete logarithm in $GF(p)$, *IEEE Transactions on Information Theory*, **31** (1985), 469–472.

[12] H. Gilbert, D. Gupta, A. M. Odlyzko, and J.-J. Quisquater; Attacks on Shamir's "RSA for paranoids," Preprint, `http://www.research.att.com/~amo/doc/recent.html`.

[13] J. L. Hafner and K. S. McCurley; A rigorous subexponential algorithm for computation of class groups, *Journal of the American Mathematical Society*, **2** (1989), 837–850.

[14] D. Hühnlein, M. J. Jacobson, Jr., S. Paulus, and T. Takagi; A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption, *Advances in Cryptology – EUROCRYPT* '98, LNCS 1403, Springer-Verlag, Berlin (1998), pp. 294–307.

[15] H. W. Lenstra, Jr.; Factoring integers with elliptic curves, *Annals of Mathematics*, **126** (1987), 649–673.

[16] A. K. Lenstra and H. W. Lenstra, Jr. (eds.); *The Development of the Number Field Sieve*, Lecture Notes in Mathematics 1554, Springer-Verlag, Berlin (1991).

[17] K. S. McCurley; A key distribution system equivalent to factoring, *Journal of Cryptology*, **1** (1988), 95–105.

[18] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone; *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL (1996).

[19] T. Okamoto; A fast signature scheme based on congruential polynomial operations, *IEEE Transactions on Information Theory*, **IT-36** (1990), 47–53.

[20] T. Okamoto and S. Uchiyama; A new public key cryptosystem as secure as factoring, *Advances in Cryptology – EUROCRYPT* '98, LNCS 1403, Springer-Verlag, Berlin (1998), pp. 308–318.

[21] R. Peralta and E. Okamoto; Faster factoring of integers of a special form, *IEICE Transactions Fundamentals*, **E79-A**(4) (1996), 489–493.

[22] R. Rivest, A. Shamir, and L. M. Adleman; A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM*, **21**(2) (1978), 120–126.

[23] R. Rivest and R. D. Silverman; Are "strong" primes needed for RSA, The 1997 RSA Laboratories Seminar Series, Seminars Proceedings (1997).

[24] R. J. Schoof; Quadratic fields and factorization, in: H. W. Lenstra and R. Tijdeman (eds.): *Computational Methods in Number Theory*, Math. Centrum Tracts 155, Part II, Amsterdam, (1983), pp. 235–286.

[25] A. Shamir; RSA for paranoids, *CryptoBytes*, **1**(3) (1995).

[26] D. Shanks; On Gauss and composition I, II, in R. A. Mollin, (ed.), *Proc. NATO ASI on Number Theory and Applications*, Kluwer Academic, Dordrecht (1989), pp. 163–179.