J. Cryptology (1988) 1: 107–118

Journal of Cryptology

A Key-Exchange System Based on Imaginary Quadratic Fields

Johannes Buchmann
Mathematisches Institut, Universität Düsseldorf, Universitätsstrasse 1, D-4000 Düsseldorf, Federal Republic of Germany

H. C. Williams
Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

Abstract. We describe another key-exchange system which, while based on the general idea of the well-known scheme of Diffie and Hellman, seems to be more secure than that technique. The new system is based on the arithmetic of an imaginary quadratic field, and makes use, specifically, of the properties of the class group of such a field.

Key words. Key-exchange system, Quadratic field, Ideal, Class group, Discrete logarithm.

1. Introduction

In [5] Diffie and Hellman described a novel scheme by which two individuals A and B could exchange a secret cryptographic key. This system had the advantage that all transmissions could be made over a public channel, and yet at the termination of this process only A and B would be in possession of the secret key.

Briefly, the idea is the following:

(i) A and B agree on a large q, where F_q is some finite field containing q elements; and some fixed primitive element g of F_q. Both q and g can be made public.
(ii) A selects an integer x at random and transmits $b = g^x$ ($b \in F_q$) to B.
(iii) B selects an integer y at random and transmits $c = g^y$ ($c \in F_q$) to A.
(iv) A determines $k = c^x$; B determines $k = b^y$ ($k \in F_q$). k is then used as the secret key.

An individual tapping the line between A and B would know g, p, b, c, but would not know x or y. If he could determine x from knowledge of g and b and the fact that $b = g^x$, then he could easily compute k. We call the problem of determining this x, given b and g, the *discrete logarithm problem.*

The values most frequently recommended for q are either 2^n or a large prime p. In his lengthy survey Odlyzko [15] suggests that a greater level of security is possible in the latter of these two possibilities.

Recently, McCurley [12] described a modified form of the Diffie–Hellman algorithm in which the field F_q is replaced by the ring $\mathbf{Z}/n\mathbf{Z}$, where n is the product of two large primes. The advantage of this scheme is that any algorithm which will break it for a nonnegligible proportion of inputs, can be used to factor n; hence, the scheme is at least as secure as it is difficult to factor n. Also, Koblitz [8] and Miller [13] have pointed out that the group of points on an elliptic curve over F_q can also be used to develop a secure key-exchange system.

The purpose of this paper is to describe yet another key exchange system. This one makes use of the properties of an imaginary quadratic field $\mathcal{K}$ and is unlike the other methods described above because no arithmetic is carried out in F_q or $\mathbf{Z}/n\mathbf{Z}$, i.e., no modular arithmetic is utilized. Instead, we conduct our arithmetic in the class group of $\mathcal{K}$. The new technique is somewhat more time consuming then those of [5] and [12]; but, on the other hand, it may be more secure than either of these schemes; comparisons are very difficult to draw. Incidentally, McCurley [12], independently of the authors, suggested the possibility of using this particular idea, but he provided no details on how it might be done.

2. Ideals on Imaginary Quadratic Fields

In this section we present several results concerning ideals in imaginary quadratic fields. Most of this material was known to Gauss; but it is usually described in the language of quadratic forms. As it is possible by using ideal theory to extend many of the theoretical and computational aspects of the material presented here to arbitrary number fields (see, for example, [1]), in the interest of possible future generalization we describe our results in terms of ideals. However, since, as mentioned above, these results are well known, we state them without proof. Proofs of most of the statements made here can be found in standard texts like Cohn [4] (see Chapters 7, 9, and 12) or Hua Loo Keng [7] (see Chapters 12 and 16).

Let $D < 0$ be a square-free integer and let $\mathcal{K} = \mathcal{Q}(\sqrt{D})$ be the imaginary quadratic field formed by adjoining $\sqrt{D}$ to the rationals $\mathcal{Q}$. If $\alpha \in \mathcal{K}$, we denote by $\bar{\alpha}$ the conjugate of α, by $\mathrm{Tr}(\alpha)$ the value of $\alpha + \bar{\alpha}$, i.e., the trace of α, and by $N(\alpha)$, the value of $\alpha\bar{\alpha}$ (≥ 0), i.e., the norm of α. Note that $|\alpha|^2 = \alpha\bar{\alpha} = N(\alpha)$.

If $\alpha, \beta \in \mathcal{K}$, we denote by $[\alpha, \beta]$ the set $\alpha\mathbf{Z} + \beta\mathbf{Z}$, where $\mathbf{Z}$ is the set of rational integers. It is well known that the ring of algebraic integers $\mathcal{O}_{\mathcal{K}}$ of $\mathcal{K}$ is given by $[1, \omega]$, where

$$\omega = (r - 1 + \sqrt{D})/r$$

and

$$r = \begin{cases} 2 & \text{when } D \equiv 1 \pmod 4, \\ 1 & \text{when } D \equiv 2, 3 \pmod 4. \end{cases}$$

If $\alpha \in \mathcal{K}$, then $\alpha \in \mathcal{O}_{\mathcal{K}}$ if and only if $\mathrm{Tr}(\alpha), N(\alpha) \in \mathbf{Z}$. Also, the discriminant $\Delta = (\omega - \bar{\omega})^2$ of $\mathcal{K}$ is given by $\Delta = 4D/r^2$.

An (integral) ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathcal{K}}$ is a subset of $\mathcal{O}_{\mathcal{K}}$ such that

(i) $\alpha + \beta \in \mathfrak{a}$ whenever $\alpha, \beta \in \mathfrak{a}$,
(ii) $\alpha\xi \in \mathfrak{a}$ whenever $\alpha \in \mathfrak{a}$, $\xi \in \mathcal{O}_{\mathcal{K}}$.

Now if $\mathfrak{a}$ is any ideal of $\mathcal{O}_{\mathscr{K}}$, then

$$\mathfrak{a} = [a, b + c\omega], \tag{2.1}$$

where $a, b, c \in \mathbf{Z}$ and $a > 0$, $c > 0$. Further, from (i) and (ii) it is easy to show that $c|a$, $c|b$, and $ac|N(b + c\omega)$. Also, if $\mathfrak{a} = [a, b + c\omega]$, where $a, b, c \in \mathbf{Z}$, $c|a$, $c|b$, and $ac|N(b + c\omega)$, then $\mathfrak{a}$ is an ideal of $\mathcal{O}_{\mathscr{K}}$. For a given $\mathfrak{a}$ the value of a in (2.1) is unique. We denote this by $L(\mathfrak{a})$; it is the least positive rational integer in $\mathfrak{a}$.

The ideal $\mathfrak{a}$ is called *primitive* when it is not divisible by any ideal except (1). Such an ideal will have $c = 1$ in (2.1).

Lemma 2.1. *If $\mathfrak{a}$ is any primitive ideal of $\mathcal{O}_{\mathscr{K}}$, then there exists some $\alpha \in \mathfrak{a}$ such that $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$ and $|\mathrm{Tr}(\alpha)| \leq L(\mathfrak{a})$.*

The next result shows that the value of $|\mathrm{Tr}(\alpha)|$ in Lemma 2.1 is unique.

Lemma 2.2. *If $\mathfrak{a}$ is an ideal of $\mathcal{O}_{\mathscr{K}}$, $\mathfrak{a} = [L(\mathfrak{a}), \alpha] = [L(\mathfrak{a}), \beta]$, and $|\mathrm{Tr}(\alpha)| \leq L(\mathfrak{a})$, $|\mathrm{Tr}(\beta)| \leq L(\mathfrak{a})$, then $|\mathrm{Tr}(\alpha)| = |\mathrm{Tr}(\beta)|$.*

An ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathscr{K}}$ is said to be *reduced* if $\mathfrak{a}$ is primitive and there does not exist a nonzero $\beta \in \mathfrak{a}$ such that $|\beta| < L(\mathfrak{a})$.

Theorem 2.3. *If $\mathfrak{a}$ is a primitive ideal of $\mathcal{O}_{\mathscr{K}}$ and $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$ with $|\mathrm{Tr}(\alpha)| \leq L(\mathfrak{a})$, then $\mathfrak{a}$ is a reduced ideal if and only if $|\alpha| \geq L(\mathfrak{a})$.*

Theorem 2.4. *If $\mathfrak{a}$ is a reduced ideal of $\mathcal{O}_{\mathscr{K}}$, then $L(\mathfrak{a}) < \sqrt{|\Delta|/3}$.*

Theorem 2.5. *If $\mathfrak{a}$ is a primitive ideal of $\mathcal{O}_{\mathscr{K}}$ and $L(\mathfrak{a}) < \sqrt{|\Delta|}/2$, then $\mathfrak{a}$ is a reduced ideal of $\mathcal{O}_{\mathscr{K}}$.*

All of these results can be proved by using the theory of binary quadratic forms once it is seen that, for $\beta \in \mathfrak{a}$, we have $\beta = xL(\mathfrak{a}) + y\alpha$ where $x, y \in Z$ and

$$4|\beta|^2 = 4N(\beta) = (2L(\mathfrak{a})x + \mathrm{Tr}(\alpha)y)^2 + |\Delta|y^2.$$

If $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathcal{O}_{\mathscr{K}}$, then

$$\mathfrak{a} = \left\{ \sum_{i=1}^{k} \xi_i \alpha_i | \xi_i \in \mathcal{O}_{\mathscr{K}} \right\}$$

is an ideal of $\mathcal{O}_{\mathscr{K}}$, where $\alpha_1, \alpha_2, \ldots, \alpha_k$, are the *generators* of $\mathfrak{a}$. We usually denote this by $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$. In fact, for any ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathscr{K}}$ we know that there exist two elements $\alpha_1, \alpha_2 \in \mathcal{O}_{\mathscr{K}}$ such that $\mathfrak{a} = (\alpha_1, \alpha_2)$, cf. (2.1): $(\alpha_1, \alpha_2) = [\alpha_1, \alpha_2]$. When $\mathfrak{a} = (\alpha)$, we say that $\mathfrak{a}$ is a *principal* ideal. When $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k)$, $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_m)$, we define the *product* ideal $\mathfrak{ab}$ by $\mathfrak{ab} = (\alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_k\beta_m)$, the ideal with the mk generators $\alpha_i\beta_j$ $(i = 1, 2, \ldots, k; j = 1, 2, \ldots, m)$. If there exist nonzero $\alpha, \beta \in \mathcal{O}_{\mathscr{K}}$ such that

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b},$$

we say that $\mathfrak{a}$ and $\mathfrak{b}$ are *equivalent* ideals of $\mathcal{O}_{\mathcal{K}}$ and denote this by $\mathfrak{a} \sim \mathfrak{b}$. This is a true equivalence relation which causes the set of all ideals in $\mathcal{O}_{\mathcal{K}}$ to be partitioned into disjoint equivalence classes. We also have

Lemma 2.6. *If* $\mathfrak{a} \sim \mathfrak{b}$, *then there exists* $\lambda \in \mathfrak{a}$ *such that* $(\lambda)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}$.

The next theorem shows that there are at most two reduced ideals in any given equivalence class of ideals.

Theorem 2.7. *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be primitive ideals of* $\mathcal{O}_{\mathcal{K}}$ *such that* $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$, $\mathfrak{b} = [L(\mathfrak{b}), \beta]$ *with* $|\mathrm{Tr}(\alpha)| \leq L(\mathfrak{a}), |\mathrm{Tr}(\mathfrak{b})| \leq L(\mathfrak{b})$. *If* $\mathfrak{a} \sim \mathfrak{b}$, *then* $L(\mathfrak{a}) = L(\mathfrak{b})$ *and* $|\mathrm{Tr}(\alpha)| = |\mathrm{Tr}(\beta)|$.

In the next section we show that each equivalence class of ideals of $\mathcal{O}_{\mathcal{K}}$ contains a reduced ideal. Indeed, we present an algorithm for finding such a reduced ideal. This can then be used as the basis of our key-exchange system.

3. The Key-Exchange Algorithm

We first point out that if $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$ is a primitive ideal of $\mathcal{O}_{\mathcal{K}}$, then so is $\mathfrak{b} = [N(\alpha)/L(\mathfrak{a}), -\bar{\alpha}]$. Further,

$$(\bar{\alpha})\mathfrak{a} = (L(\mathfrak{a}))\mathfrak{b};$$

hence, $\mathfrak{a} \sim \mathfrak{b}$.

Algorithm 3.1.

1. *For a given primitive ideal* $\mathfrak{a} = \mathfrak{a}_1 = [L(a), \alpha]$ *of* $\mathcal{O}_{\mathcal{K}}$, *put* $Q_0 = rL(\mathfrak{a})$ (> 0), $P_0 = r\alpha - \sqrt{D} \in \mathbf{Z}$. *The value of* r *here is that defined in Section* 2.
2. *Compute*

$$\begin{cases} q_i = Ne(P_i/Q_i), \\ P_{i+1} = q_iQ_i - P_i, \\ Q_{i+1} = (P_{i+1}^2 - D)/Q_i, \end{cases} \tag{3.1}$$

   where by $Ne(\gamma)$ *we denote an integer such that* $|\gamma - Ne(\gamma)| \leq \frac{1}{2}$. (*Unique unless* $x = \pm\frac{1}{2}$.)
3. $$\mathfrak{a}_{i+1} = [Q_i/r, P_i + \sqrt{D})/r]$$

   is a reduced ideal of $\mathcal{O}_{\mathcal{K}}$ *when*

$$Q_{i+1} \geq Q_i.$$

Proof. By (3.1) we have

$$\mathfrak{a}_{j+1} = [Q_j/r, (P_j + \sqrt{D})/r] = [Q_j/r, (-P_{j+1} + \sqrt{D})/r].$$

Thus, by the remark preceding this algorithm and the formulas of (3.1), we see that if $\mathfrak{a}_{j+1}$ is an ideal, then so is $\mathfrak{a}_{j+2}$ and $\mathfrak{a}_{j+2} \sim \mathfrak{a}_{j+1}$. Further, if $\alpha_{i+1} = (-P_{i+1} + \sqrt{D})/r$,

then $|\mathrm{Tr}(\alpha_{i+1})| = |2P_{i+1}/r| = 2|q_iQ_i - P_i|/r = 2Q_i|q_i - P_i/Q_i|/r \leq Q_i/r = L(\mathfrak{a}_{i+1})$. It follows from Theorem 2.3 that $\mathfrak{a}_{i+1}$ is reduced when $N(\alpha_{i+1}) \geq L(\mathfrak{a}_{i+1})^2$, that is when $Q_{i+1} \geq Q_i$. □

To provide greater ease in computation we can modify Algorithm 3.1 as follows. We first put $T_0 = |P_0|$, $t_0 = P_0/T_0$, and $Q_{-1} = (P_0^2 - D)/Q_0$. It is then easy to show that Step 2 of Algorithm 3.1 can be reformulated as

$$s_i = [T_i/Q_i],$$
$$R_i = \text{remainder on dividing } T_i \text{ by } Q_i,$$
$$M_i = Q_i - 2R_i.$$

If $M_i \geq 0$, then

$$T_{i+1} = R_i,$$
$$Q_{i+1} = Q_{i-1} - s_i(R_i + T_i),$$
$$t_{i+1} = -t_i;$$

if $M_i < 0$, then

$$T_{i+1} = R_i + M_i,$$
$$Q_{i+1} = Q_{i-1} - s_i(R_i + T_i) + M_i,$$
$$t_{i+1} = t_i.$$

In this formulation we have P_j in (3.1) given by $P_j = t_jT_j$ for any $j \geq 0$.

We must next show that we ultimately get some i such that $Q_{i+1} \geq Q_i$. We do this in

Theorem 3.2. *If* $\mathfrak{a}$ *is given as in Algorithm* 3.1, *then we get* $Q_{i+1} \geq Q_i$ *for some* $i \leq 2 + [\frac{1}{2}\log_2(3Q_0/5\sqrt{|D|})]$.

Proof. We first note that

$$0 < Q_{j+1} \leq ((Q_j/2)^2 + |D|)/Q_j = Q_j/4 + |D|/Q_j.$$

If we define $\rho_j = Q_j/\sqrt{|D|}$, then

$$\rho_{j+1} \leq \rho_j/4 + 1/\rho_j. \tag{3.2}$$

Also, if $K_j = (5 \cdot 4^j + 1)/3$, then for $j > 1$ it is easy to show that

$$K_j/4 + 1/K_{j-1} < K_{j-1}. \tag{3.3}$$

Now if $2 < \rho_i < K_1 = 7$, then by (3.2) it is clear that $\rho_{i+1} < K_0 = 2$ when $\rho_i > 4$ and $\rho_{i+1} < \frac{3}{2}$ when $\rho_i \leq 4$. Thus, by using (3.2) and (3.3) we see that $\rho_{i+1} \leq K_{j-1}$ when $2 < \rho_i < K_j$ $(j > 0)$. It follows that if $\rho_0 < K_m$, then $\rho_t < K_0 = 2$ for some $t \leq m$. Putting $m = [\frac{1}{2}\log_2(3\rho_0/5)] + 1$, we have

$$K_m > \rho_0 + \tfrac{1}{3} > \rho_0;$$

thus, for some $i \leq 1 + [\frac{1}{2}\log_2(3Q_0/5\sqrt{|D|})]$, we have $Q_i < 2\sqrt{|D|}$.

Suppose $Q_i < 2\sqrt{|D|}$. If $Q_{i+1} \geq Q_i$, then $\mathfrak{a}_{i+1}$ is reduced. If $Q_{i+1} < Q_i$, then $\mathfrak{a}_{i+1}$ is not a reduced ideal, and as a consequence there must exist some nonzero $\gamma \in \mathfrak{a}_{i+1}$ such that $|\gamma|$ is minimal and $|\gamma| < Q_i/r$. Further, by Theorem 2.5 $Q_i/r > \sqrt{|\Delta|}/2$. Since

$$r^2|\gamma|^2 = (xQ_i + yP_i)^2 + |D|y^2 \qquad (x, y \in \mathbf{Z}),$$

we must have $|y| = 1$. If $M = \min\{|xQ_i \pm P_i| | x \in \mathbf{Z}\}$, then $r^2|\gamma|^2 = M^2 + D$, where $M = |P_{i+1}| = |q_iQ_i - P_i| \leq Q_i/2$; hence, we can put $\gamma = (-P_{i+1} + \sqrt{D})/r$. Since $\mathfrak{a}_{i+1} = [Q_i/r, \gamma]$, we must have $\mathfrak{a}_{i+2} = [Q_{i+1}/r, (P_{i+1} + \sqrt{D})/r]$ a reduced ideal of $\mathcal{O}_\mathscr{K}$. For if $\mathfrak{a}_{i+2}$ is not reduced, there must exist some $\beta \in \mathfrak{a}_{i+2}$ such that

$$N(\beta) < L(\mathfrak{a}_{i+2})^2 = N(\gamma)/L(\mathfrak{a}_{i+1})^2$$

and

$$L(\mathfrak{a}_{i+1})\beta = \overline{\gamma}\lambda \qquad \text{for some} \quad \lambda \in \mathfrak{a}_{i+1}.$$

Since $N(\beta) = N(\gamma)N(\lambda)/L(\mathfrak{a}_{i+1})^2$, we get $N(\lambda) < N(\gamma)$, which, by selection of γ, is impossible. Since $\mathfrak{a}_{i+2}$ is a reduced ideal we must also have $Q_{i+2} \geq Q_{i+1}$. The theorem now follows easily from our earlier bound on i. □

This result is similar to that presented by Lagarias [9]; however, we have used a somewhat different manner of proof here.

We can now set up a method similar to that of [5] for a secret key exchange. Two users A and B select a value of D such that $|D|$ is large ($\approx 10^{200}$) and an ideal $\mathfrak{a}$ in $\mathcal{O}_\mathscr{K}$. The value of D and the ideal $\mathfrak{a}$ can be made public.

(1) A selects at random an integer x and computes a reduced ideal $\mathfrak{b}$ such that

$$\mathfrak{b} \sim \mathfrak{a}^x.$$

A sends $\mathfrak{b}$ to B.

(2) B selects at random an integer y and computes a reduced ideal $\mathfrak{c}$ such that

$$\mathfrak{c} \sim \mathfrak{a}^y.$$

B sends $\mathfrak{c}$ to A.

(3) A computes a reduced ideal $\mathfrak{k}_1 \sim \mathfrak{c}^x$; B computes a reduced ideal $\mathfrak{k}_2 \sim \mathfrak{b}^y$.

Since $\mathfrak{k}_1 \sim \mathfrak{c}^x \sim (\mathfrak{a}^y)^x = (\mathfrak{a}^x)^y \sim \mathfrak{b}^y \sim \mathfrak{k}_2$, we see by Theorem 2.7 that $L(\mathfrak{k}_1) = L(\mathfrak{k}_2)$ and if $\mathfrak{k}_1 = [L(\mathfrak{k}_1), \kappa_1]$, $\mathfrak{k}_2 = [L(\mathfrak{k}_2), \kappa_2]$, then $|\mathrm{Tr}(\kappa_1)| = |\mathrm{Tr}(\kappa_2)|$. Thus A and B can either use $L(\mathfrak{k}_1) = L(\mathfrak{k}_2)$ or $|\mathrm{Tr}(\kappa_1)| = |\mathrm{Tr}(\kappa_2)|$ or parts thereof as their secret key. It should, however, be borne in mind that since $L(\mathfrak{k}_1)|N(\kappa_1)$, the values of $L(\mathfrak{k}_1)$ and $\mathrm{Tr}(\kappa_1)$ are not independent.

Indeed, this idea can also be converted into a public-key cryptosystem in a manner similar to that proposed by El Gamal [6]. If A wishes to send a secure meassage m to B, he can compute for randomly selected x, $\mathfrak{k} \sim \mathfrak{c}^x$, where $\mathfrak{k}$ is a reduced ideal and $\mathfrak{c} \sim \mathfrak{a}^y$ is in B's public file or has been sent to A by B. (Here, as before, x is known only to A and y is known only to B). The encrypted message is sent to B as $(M + L(\mathfrak{k}), \mathfrak{b})$, where $\mathfrak{b} \sim \mathfrak{a}^x$ and M is the first block of m with $M < L(\mathfrak{k})$. Subsequent blocks of m would be sent in the same way, although A must change x for each new block he sends. To find M, B must determine $L(\mathfrak{k})$; however, since he has

$\mathfrak{b} \sim \mathfrak{a}^x$ and y he can compute

$$\mathfrak{b}^y \sim \mathfrak{a}^{xy} \sim \mathfrak{c}^x \sim \mathfrak{k}.$$

It remains to consider the problem of finding an efficient algorithm for multiplication of ideals. The binary method of exponentiation will then provide an efficient algorithm for computing $\mathfrak{a}^m$ for large m. We first point out that if $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals of $\mathcal{O}_{\mathcal{K}}$, then we can find an ideal $\mathfrak{c}$ of $\mathcal{O}_{\mathcal{K}}$ and $U \in \mathbf{Z}$ such that

$$(U)\mathfrak{c} = \mathfrak{a}\mathfrak{b} \tag{3.4}$$

by using the algorithm mentioned in Shanks [22]. If $\mathfrak{a} = [Q/r, (P + \sqrt{D})/r]$, $\mathfrak{b} = [Q'/r, (P' + \sqrt{D})/r]$, then in (3.4)

$$U = \gcd((P + P')/r, Q/r, Q'/r)$$

and $\mathfrak{c} = [Q''/r, (P'' + \sqrt{D})/r]$. We find Q'', P'' by first solving

$$(Q/r)x_1 \equiv G \pmod{Q'/r},$$

where $G = \gcd(Q/r, Q'/r)$, for $x_1 \pmod{Q'/r}$. We then put $U = \gcd(G, (P + P')/r)$ and solve

$$x_2(P + P')/r + Gy_2 = U$$

for x_2, y_2. Then

$$Q'' \equiv QQ'/(rU^2),$$

$$P'' \equiv P + XQ/(rU) \pmod{Q''},$$

where

$$X \equiv y_2x_1(P' - P) + x_2(D - P^2)/Q \pmod{Q'/U}.$$

In certain cases we can simplify this. For example, when $G = 1$, we get $U = 1$, $x_2 = 0$, $y_2 = 1$; hence,

$$X \equiv x_1(P' - P) \pmod{Q'}.$$

In the special case of $\mathfrak{a} = \mathfrak{b}$, i.e., $Q' = Q$, $P' = P$, we get $U = \gcd(Q/r, 2P/r)$, $x_1 = 0$,

$$(2P/r)x_2 \equiv U \pmod{Q/r}$$

and

$$X \equiv x_2(D - P^2)/Q \pmod{Q/U}.$$

If $m = (b_0\ b_1\ b_2\ \cdots\ b_k)_2$ is the base 2 (binary) representation of m ($b_0 = 1$), then let $\mathfrak{s}_0 \sim \mathfrak{a}$ and define $\mathfrak{t}_i \sim \mathfrak{s}_i^2$ and

$$\mathfrak{s}_{i+1} \sim \begin{cases} \mathfrak{t}_i, & b_{i+1} = 0, \\ \mathfrak{t}_i\mathfrak{a}, & b_{i+1} = 1, \end{cases}$$

where $\mathfrak{t}_i$ and $\mathfrak{s}_{i+1}$ are reduced ideals of $\mathcal{O}_{\mathcal{K}}$. It is easy to see that $\mathfrak{s}_k \sim \mathfrak{a}^m$. If we select $\mathfrak{a}$ such that $L(\mathfrak{a})$ is a prime $> \sqrt{|\Delta|/3}$, then for all of the multiplications $\mathfrak{t}_i\mathfrak{a}$ we would likely have $\gcd(L(\mathfrak{t}_i), L(\mathfrak{a})) = 1$. As we have seen above, this simplifies somewhat the determination of $\mathfrak{s}_{i+1}$. In any event we see that to compute $\mathfrak{s}_k$ requires the performance of $O(\log m \log|D|)$ elementary operations.

In the next section we describe the security of our proposed key-exchange system.

4. Security of the Scheme

From the results of the previous section we see that the complexity of this key-exchange system is greater than that of [5] and so is the bandwidth. That is, to communicate about 100 digits of key, it is necessary to exchange about 200 digits of information across the communication channel. Thus, to compensate for this extra effort, we would like our scheme to be more secure than that of [5]. While we cannot formally prove this here, we can provide results which suggest that this is the case.

That there can only be a finite number of equivalence classes of ideals in $\mathcal{O}_{\mathcal{K}}$ follows from the results of Section 3 and Theorem 2.4. We denote this number by h and call h the *class number* of $\mathcal{K}$. If $\mathcal{C}_1$ and $\mathcal{C}_2$ are two of these equivalence classes, we define the product $(\mathcal{C}_1\mathcal{C}_2)$ of these classes by

$$\mathcal{C}_3 = \mathcal{C}_1\mathcal{C}_2 = \{\mathfrak{c} = \mathfrak{a}\mathfrak{b} | \mathfrak{a} \in \mathcal{C}_1, \mathfrak{b} \in \mathcal{C}_2\}.$$

Under this product operation, it can be shown that the set of all equivalence classes of ideals of $\mathcal{O}_{\mathcal{K}}$ forms an abelian group $\mathbf{G}$ of order h with identity the class of principal ideals.

We know (see p. 389 of [14]) that

$$h \leq \frac{2}{\pi}|\Delta|^{1/2}(1 + \log(2|\Delta|^{1/2}/\pi))$$

and that for any $\varepsilon > 0$

$$h > |\Delta|^{1/2-\varepsilon}$$

for all sufficiently large Δ. Indeed under the Extended Riemann Hypothesis (ERH) Littlewood [11] has shown that

$$\frac{\pi(1 + o(1))\sqrt{|\Delta|}}{12e^{\gamma} \log\log|\Delta|} < h < \frac{2(1 + o(1))\sqrt{|\Delta|} \log\log|\Delta|}{\pi}.$$

We can replace the $1 + o(1)$ here by absolute constants by using the explicit results of Oesterlé [16]. Thus, we would expect h to be of about the same order of magnitude as $|\Delta|^{1/2}$.

Suppose a cryptanalyst who is attempting to break our system has at his disposal the value of D, and the ideals, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ but does not know x or y; his problem is to determine $\mathfrak{k}_1$ or $\mathfrak{k}_2$. One way he might approach this is to attempt to solve the discrete logarithm problem in $\mathbf{G}$; that is, given a reduced ideal $\mathfrak{a}$ and a reduced ideal $\mathfrak{b}$ such that $\mathfrak{b} \sim \mathfrak{a}^x$, find x.

One simple attack (the giant-step–baby-step method of [21]) is to put $q = Ne(|D|^{1/4})$ and assume that $x = qk - r$, where $0 \leq r < q$. Since we can also assume that $h > x$, and we know that $h = O(|\Delta|^{1/2+\varepsilon})$, we see that $k = O(|\Delta|^{1/4+\varepsilon})$. We first compute $\mathfrak{f} \sim \mathfrak{a}^q$. We then find all the $O(|\Delta|^{1/4+\varepsilon})$ reduced ideals equivalent to $\mathfrak{a}^j\mathfrak{b}$ for $j = 0, 1, 2, \ldots, q-1$ and check for when $\mathfrak{f}^i$, $i = 1, 2, \ldots$, is one of these. Since $k = O(|\Delta|^{1/4+\varepsilon})$, we find i, j such that $\mathfrak{f}^i = \mathfrak{a}^j\mathfrak{b}$ in $O(|\Delta|^{1/4+\varepsilon})$ operations. When this occurs we have $x = qi - j$. We note here that for the complexity result given above to hold we must sort the list of reduced ideals equivalent to $\mathfrak{a}^j\mathfrak{b}$ $(j = 0, \ldots, q-1)$. In practice, however, it is more efficient to use hashing techniques.

The method of Pohlig and Hellman [17] can be adapted to the solution of this problem. Indeed, we can regard this technique as a more sophisticated version of the giant-step–baby-step method. If p is the largest prime factor of h, then this algorithm will find x in $O(p^{1/2+\varepsilon})$ operations, utilizing about the same amount of storage. However, in order to employ this scheme, we must know the value of h. The fastest known methods of determining h are of complexity $O(|\Delta|^{1/5+\varepsilon})$ (see [10] and [21]), assuming the ERH, even when h is made up exclusively of small prime factors.

The index calculus method (see [15]) has proved to be a very successful method for attacking the discrete logarithm problem; however, it appears to be rather difficult to apply to our scheme. The reason for this is that we must first determine what the order of $\mathscr{C}$, the class which contains $\mathfrak{a}$, is in the class group. This, of course, is in a sense begging the question. We do not know how to do that efficiently.

It appears then that the problem of determining x such that $\mathfrak{b} \sim \mathfrak{a}^x$ is a very difficult one. The best-known methods are of complexity $O(|\Delta|^{1/4+\varepsilon})$ or possibly $O(|\Delta|^{1/5+\varepsilon})$. Just how difficult the problem really is, is not known. However, by using the ideas of Shanks [22], we can show that if an efficient method for solving the problem is discovered, then this method will very likely allow us to factor D. This suggests that the problem of finding x is at least as difficult as the factoring problem.

If $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$ is any ideal of $\mathcal{O}_{\mathscr{K}}$, define $\bar{\mathfrak{a}}$ to be the ideal $[L(\mathfrak{a}), \bar{\alpha}]$. We say that $\mathfrak{a}$ is an *ambiguous* ideal of $\mathcal{O}_{\mathscr{K}}$ if $\mathfrak{a} = \bar{\mathfrak{a}}$. Note that if $\mathfrak{a}$ is ambiguous, then $\alpha + \bar{\alpha} \in \mathfrak{a}$; hence, $L(\mathfrak{a})|\mathrm{Tr}(\alpha)$. If $|\mathrm{Tr}(\alpha)| \leq L(\mathfrak{a})$, we must have $|\mathrm{Tr}(\alpha)| = L(\mathfrak{a})$. If $\mathfrak{a}$ is primitive and ambiguous, then since $4N(\alpha) = |\mathrm{Tr}(\alpha)|^2 + D$, we see that $L(\mathfrak{a})|D$.

If $\mathfrak{b}^2 \sim (1)$, then $\mathfrak{b}^2 = (\beta)$ for some $\beta \in \mathcal{O}_{\mathscr{K}}$. Putting $\gamma = L(\mathfrak{b}) + \bar{\beta}$, it is a simple matter to show that $\bar{\beta}\bar{\gamma} = L(\mathfrak{b})\gamma$; thus, when $\mathfrak{c} = (\gamma)\mathfrak{b}$, we get $\mathfrak{c} = \bar{\mathfrak{c}}$. That is, if $\mathfrak{b}^2 \sim (1)$, we must have an ambiguous ideal in the class of $\mathfrak{b}$.

If $s|D$ $(s > 0)$, then $[s, \sqrt{D}]$ is an ambiguous ideal when $r = 1$; further, by Theorem 2.5 $[s, \sqrt{D}]$ is a reduced ideal when $s < \sqrt{|D|}$. When $r = 2$, $[s, (s + \sqrt{D})/2]$ is an ambiguous ideal; also, if $s < \sqrt{|D|/3}$, then $N((s + \sqrt{D})/2) \geq s^2$ and $[s, (s + \sqrt{D})/2]$ must be a reduced ideal by Theorem 2.3. If $\sqrt{|D|} > s > \sqrt{|D|/3}$, we can use Algorithm 3.1 to show that

$$\mathfrak{a} = [(t + s)/4, ((s - t)/2 + \sqrt{D})/2]$$

is a reduced ideal such that $|\mathrm{Tr}(\alpha)| \leq L(\mathfrak{a})$, where $\alpha = ((s - t)/2 + \sqrt{D})/2$.

From these remarks and Theorem 2.7 it follows that if $\mathfrak{a}$ is a reduced ideal equivalent to an ambiguous ideal, then either $L(\mathfrak{a})$ or $2L(\mathfrak{a}) + |\mathrm{Tr}(\alpha)|$ is a factor of D when $\mathfrak{a} = [L(\mathfrak{a}), \alpha]$ and $|\mathrm{Tr}(\alpha)| \leq L(\mathfrak{a})$. Also, this factor will be a nontrivial factor of D if $\mathfrak{a}$ is not principal. We further remark that if D is a composite integer, there must be an equivalence class of ideals which contains a nonprincipal ambiguous ideal; hence, since $\mathfrak{a}^2 = \mathfrak{a}\bar{\mathfrak{a}} = (L(\mathfrak{a}))$ when $\mathfrak{a}$ is a primitive ambiguous ideal, we must have $2|h$.

Now assume that D is a composite integer and we can solve the problem of finding x for a given $\mathfrak{a}$, $\mathfrak{b}$ such that $\mathfrak{b} \sim \mathfrak{a}^x$. Since $2|h$, the probability that, for $\mathfrak{b} = (1)$, the value of x is such that $2|x$ is at least $1/2$. If we can find x, then for $m = x/2$ we have $(\mathfrak{a}^m)^2 \sim (1)$. It follows that there must exist an ambiguous ideal $\mathfrak{c} \sim \mathfrak{a}^m$ and that a reduced ideal equivalent to $\mathfrak{c}$ will with probability $\geq 1/2$ provide us with a nontrivial factorization of D.

Of course, it might be possible to cryptanalyze our scheme without having to

solve the discrete logarithm problem in **G**. For suppose that A is some algorithm that on being given $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, with $\mathfrak{b} \sim \mathfrak{a}^x$, $\mathfrak{c} \sim \mathfrak{a}^y$, produces $\mathfrak{f} = A(\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$, where $\mathfrak{f} \sim \mathfrak{a}^{xy}$. By using ideas similar to those developed by Schmuely [20] and McCurley [12], we can show that if a cryptanalyst possesses such an algorithm, then it is very likely that he can easily find a nontrivial factor of D.

We assume as before that D is composite. Let S_2 be the Sylow 2-subgroup of **G** and let $2^m \| h$. Now S_2 can be written as a direct product of cyclic groups $C(m_i)$ with $m_i | 2^m$ $(i = 1, 2, \ldots, t)$, i.e.,

$$S_2 = C(m_1) \times C(m_2) \times \cdots \times C(m_t).$$

If $2^j = \max\{m_1, m_2, \ldots, m_t\} \geq 2$ and $s = h/2^m$, then for any ideal class $\mathscr{C}$ in **G** we have

$$\mathscr{C}^{2^j s} = 1; \tag{4.1}$$

further, there must exist an ideal class $\mathscr{E}$ in G such that

$$\mathscr{E}^{2^j} = 1 \quad \text{and} \quad \mathscr{E}^{2^{j-1}} \neq 1.$$

Thus, if $\mathscr{C}^{2^{j-1}s} = 1$, then $(\mathscr{C}\mathscr{E})^{2^{j-1}s} \neq 1$ and it follows that at least half of the ideal classes in **G** possess the property that if $\mathscr{C}$ is such a class, then $\mathscr{C}^{2^{j-1}}$ is of even order.

Let $\mathscr{C}$ be any element of G and $s = 2u - 1$. By (4.1) we have

$$\mathscr{C}^{2^{j+1}u} = \mathscr{C}^{2^j}. \tag{4.2}$$

Hence, the subgroups of G generated by $\mathscr{C}^{2^j}$ and $\mathscr{C}^{2^{j+1}}$ are identical. By our previous remarks we see that if we select at random an ideal $\mathfrak{g}$ of $\mathcal{O}_{\mathscr{K}}$, then with probability $\geq 1/2$, we will find that $g^{2^{j-1}v}$ is not principal whenever v is odd. For such a $\mathfrak{g}$ put $\mathfrak{a} \sim \mathfrak{g}^{2^{j+1}}$, select odd x, y at random, and put $\mathfrak{b} \sim \mathfrak{g}^{2^j x}$, $\mathfrak{c} \sim \mathfrak{g}^{2^j y}$. By (4.2) we have

$$\mathfrak{b} \sim \mathfrak{g}^{2^j x} \sim \mathfrak{g}^{2^{j+1}xu} \sim \mathfrak{a}^{xu},$$

$$\mathfrak{c} \sim \mathfrak{g}^{2^j y} \sim \mathfrak{g}^{2^{j+1}yu} \sim \mathfrak{a}^{yu};$$

thus, we may use algorithm A to produce

$$\mathfrak{f} = A(\mathfrak{a}, \mathfrak{b}, \mathfrak{c}) \sim \mathfrak{a}^{xyu^2} \sim \mathfrak{g}^{2^{j+1}xyu^2}. \tag{4.3}$$

Now

$$2^{j+1}u^2 \equiv 2^{j-1}s^2 + 2^{j-1} \pmod{2^j s};$$

hence, by (4.1) and (4.3) we have

$$\mathfrak{f} \sim \mathfrak{g}^{2^{j-1}s^2xy}\mathfrak{g}^{2^{j-1}xy}$$

and

$$\mathfrak{f}^2 \sim \mathfrak{g}^{2^j xy}.$$

If

$$\mathfrak{g}^{2^{j-1}xy} \sim \mathfrak{f},$$

then

$$\mathfrak{g}^{2^{j-1}s^2xy} \sim (1),$$

which, by selection of $\mathfrak{g}$, is not possible (s^2xy is odd); thus,

$$\mathfrak{d} = \mathfrak{f}\bar{\mathfrak{g}}^{2^{j-1}xy}$$

is not a principal ideal, but $\mathfrak{d}^2 \sim (1)$. Also, we can compute $\mathfrak{d}$ by making a call to $A(\mathfrak{g}^{2^{s-1}}, \mathfrak{g}^{2^{s-1}x}, \mathfrak{g}^{2^{s-1}y})$ to find $\mathfrak{g}^{2^{j-1}xy}$. As we have seen above, the knowledge of such an ideal $\mathfrak{d}$ provides us with information that allows us to factor D very easily. It might be argued that we need to know the value of j here, but since $j \leq \log_2 h = O(\log D \log\log D)$, there is no difficulty in attempting to guess its value. In many special cases (see below) we can obtain much better bounds on j.

One other problem that might arise in our scheme is that the order of the class $\mathscr{C}$ of $\mathfrak{a}$ might be very small. However, this seems to be most unlikely. Recently, Cohen and Lenstra [3] presented several heuristic results concerning the class group of $\mathscr{K}$. We list some of those below:

(a) The probability that the odd part of the class group is cyclic is

$$97.757\%.$$

(b) If m is any odd integer, the probability that m divides h is

$$\prod_{p^\alpha \| m} \left\{ 1 - \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right) \Big/ \prod_{i=1}^{\alpha-1} \left(1 - \frac{1}{p^i}\right) \right\}.$$

(c) If e is a fixed odd integer, the average number of elements of the class group which are of order exactly e is 1.

(d) If p is an odd prime and r_p the p rank of the class group, then the probability that $r_p = a$ given r is

$$p^{-r^2} \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right) \Big/ \prod_{i=1}^{r} \left(1 - \frac{1}{p^i}\right)^2.$$

Extensive numerical results of Buell [2] tend to confirm these heuristics.

Now if λ is the number of distinct prime divisors of Δ, it is known that $2^{\lambda-1} | h$. For many values of D we can guarantee $2^\lambda \nmid h$ by using results of Rédei [18]. For example, if $D = -p_1 p_2 \equiv 1 \pmod 4$, where p_1, p_2 are primes such that the Legendre symbol $(p_1/p_2) = -1$, then $4 \nmid h$. Thus, we can select many values of D such that the exact power of 2 which divides h is small. For such D values we would expect the class group to be cyclic or nearly so. Since in a cyclic group of order m, there exist $\varphi(d)$ generators for any subgroup of order $d | m$ and

$$\frac{\varphi(d)}{d} > \left(e^\gamma \log\log d + \frac{2.50367}{\log\log d} \right)^{-1}$$

(see (3.42) of [19]), the chance of selecting an ideal $\mathfrak{a}$ such that $\mathscr{C}$ has small order is very small when h is large.

References

[1] Johannes Buchmann and H. C. Williams, On principal ideal testing in algebraic number fields, *J. Symbolic Comput.* **4** (1987), 11–19.

[2] D. A. Buell, The expectation of success using a Monte-Carlo factoring method—some statistics on quadratic class numbers, *Math. Comp.* **43** (1984), 313–327.

[3] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups of number fields, *Number Theory* (Noordwijkerhout, 1983), Lecture Notes in Mathematics, vol. 1068, Springer-Verlag, Berlin, 1984, pp. 33–62.

[4] H. Cohn, *Advanced Number Theory*, Dover, New York, 1980.
[5] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory* **22** (1976), 472–492.
[6] T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory* **31** (1985), 469–472.
[7] Hua Loo Keng, *Introduction to Number Theory*, Springer-Verlag, Berlin, 1982.
[8] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.* **48** (1987), 203–209.
[9] J. Lagarias, Worst-case complexity bounds for algorithms in the theory of integral quadratic forms, *J. Algorithms* **1** (1980), 142–186.
[10] H. W. Lenstra, Jr., *On the calculation of Regulators and Class Numbers of Quadratic Fields*, London Mathematical Society Lecture Notes Series, vol. 56, Cambridge University Press, Cambridge, 1982, pp. 123–150.
[11] J. E. Littlewood, On the class number of the corpus $P(\sqrt{-k})$, *Proc. London Math. Soc.* **27** (1928), 358–372.
[12] K. S. McCurley, *A Key Distribution System Equivalent to Factoring*, preprint, June 1987.
[13] V. Miller, Use of elliptic curves in cryptosystems, *Advances in Cryptology* (Proceedings of Crypto '85), Lecture Notes in Computer Science, vol. 218, Springer-Verlag, New York, 1986, pp. 417–426.
[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Warsaw, 1974.
[15] A. Odlyzko, Discrete logarithms in finite fields and their cryptographic significance, *Advances in Cryptology* (Proceedings of Eurocrypt '84), Lecture Notes in Computer Science, vol. 209, Springer-Verlag, New York, 1985, pp. 224–314.
[16] J. Oesterlé, Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisée, *Astérisque* **61** (1979), 165–167.
[17] S. Pohlig and M. Hellman, An improved algorithm for computing discrete logarithms over GF(p) and its cryptographic significance, *IEEE Trans. Inform. Theory* **24** (1978), 106–110.
[18] L. Rédei, Über die Klassenzahl des imaginären quadratischen Zahlkörpers, *J. Reine Angew. Math.* **159** (1928), 210–219.
[19] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.
[20] Z. Schmuely, Composite Diffie–Hellman public-key generating schemes are hard to break, Technical Repart No. 356, Computer Science Department, Technion-Israel Institute of Technology, February 1985.
[21] R. Schoof, Quadratic fields and factorization, *Computational Methods in Number Theory*, Math Centrum Tracts, Number 155, Part II, Amsterdam, 1983, pp. 235–286.
[22] D. Shanks, *Class Number, a Theory of Factorization, and Genera*, Proceedings of Symposia in Pure Mathematics, vol. 20, AMS. Providence, RI, 1971, pp. 415–440.