A key exchange system based on real quadratic fields
Extended abstract

Johannes A. Buchmann
FB 10–Informatik
Universität des Saarlandes
6600 Saarbrücken
West Germany

Hugh C. Williams
Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada R3T2N2

1 Introduction

In [3] Diffie and Hellman described a novel scheme by which two individuals could exchange a secret cryptographic key over a public channel. This scheme is based on the arithmetic in the multiplicative group $F^\times$ of a finite field F. It is secure because computing discrete logarithms in finite fields is a very hard problem. It has been noted subsequently by several authors (e.g. [1], [5], [6]) that any finite abelian group G may be used to replace $F^\times$ in this scheme as long as the discrete logarithm problem in G is difficult.

In this paper we will for the first time present a Diffie-Hellman key exchange protocol based on a finite subset of an infinite abelian group, which is not a subgroup, namely on the set $\mathcal{R}$ of reduced principal ideals of a real quadratic order. Currently, the best known algorithms for breaking this scheme are exponential in the size of the key. Moreover, the problem of breaking the s cheme is closely related to the very difficult problems of computing class numbers of real quadratic orders and factoring large integers.

2 The idea

Let D be a positive integer which is not a square, $D \equiv 0, 1 \bmod 4$. Let

$$K = \mathcal{Q} + \mathcal{Q}\sqrt{D}$$

be the *real quadratic number field* generated by $\sqrt{D}$. For $\xi = x + y\sqrt{D}$, $x, y \in \mathcal{Q}$, we denote by $\xi' = x - y\sqrt{D}$ its algebraic conjugate. Let

$$\mathcal{O} = \mathcal{Z} + \mathcal{Z}\frac{D + \sqrt{D}}{2}$$

be the *real quadratic order* of discriminant D. A number $\mu \in \mathcal{O}$ is called a *minimum* of $\mathcal{O}$ if $\mu > 0$ and if there is no $\alpha \neq 0$ in $\mathcal{O}$ with $|\alpha| < \mu$ and $|\alpha'| < |\mu'|$. The set of minima in $\mathcal{O}$ is denoted by M. A *principal ideal* of $\mathcal{O}$ is a subset of K of the form $\mathfrak{a} = \frac{1}{\alpha}\mathcal{O}$ with $\alpha \in K^{\times}$. Such an ideal is called *reduced* if $\alpha \in M$. Denote the set of principal ideals of $\mathcal{O}$ by $\mathcal{P}$ and the set of reduced principal ideals of $\mathcal{O}$ by $\mathcal{R}$. Each $\mathfrak{a} \in \mathcal{R}$ has a presentation

$$\mathfrak{a} = \mathcal{Z} + \mathcal{Z}\frac{b+\sqrt{D}}{2a} \tag{1}$$

where $a, b \in \mathcal{Z}$, $0 < a < \sqrt{D}$ and $0 \leq b < 2a$. In our key exchange protocol the communication partners will agree on a reduced ideal which will serve as the secret key. Unfortunately, $\mathcal{R}$ does not carry a group structure and therefore, the ideas of Buchmann/Williams [1] cannot be used in this context. Instead, we will use the infrastructure idea of Shanks [9] which basically tells us that $\mathcal{R}$ is "almost" a group.

It can easily be shown that the set

$$\{\log \mu : \mu \in M\}$$

is discrete on the real line R. Hence, we can arrange the minima of $\mathcal{O}$ in a two sided sequence $(\mu_j)_{j\in\mathcal{Z}}$ which is defined by the two properties

$$\mu_0 = 1 \quad \text{and} \quad (\mu_i < \mu_j \Leftrightarrow i < j).$$

Correspondingly, we put $\mathfrak{a}_j = \frac{1}{\mu_j}\mathcal{O}$ for $j \in \mathcal{Z}$. Then we have

$$\mathcal{R} = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_p\}$$

for some $p \in \mathcal{Z}_{\geq 1}$ which is chosen such that $\mathfrak{a}_i = \mathfrak{a}_j \Leftrightarrow i \equiv j \bmod p$. For any $x \in R$ and for any $\mathfrak{a} \in \mathcal{P}$ we define the *distance* $\delta(\mathfrak{a}, x)$ of $\mathfrak{a}$ and x as follows: let $\alpha \in K_{>0}$ such that $\frac{1}{\alpha}\mathcal{O}r = \mathfrak{a}$ and $|x - \log\alpha|$ is minimum. Put $\delta(\mathfrak{a}, x) = x - \log\alpha$. We denote by $\hat{\delta}(\mathfrak{a}, x)$ the approximation to $\delta(\mathfrak{a}, x)$ which is actually computed in our scheme. We say that $\mathfrak{a} \in \mathcal{P}$ is *on the left (on the right)* of x if $\delta(\mathfrak{a}, x) > (<)0$. We say that $\mathfrak{a} \in \mathcal{P}$ is *closer* to x than $\mathfrak{b} \in \mathcal{P}$ if $|\delta(\mathfrak{a}, x)| < |\delta(\mathfrak{b}, x)|$. We denote by $\mathfrak{a}_+(x)$ the closest reduced principal ideal on the right of x, by $\mathfrak{a}_-(x)$ the closest reduced principal ideal on the left of x, and by $\mathfrak{a}(x)$ the reduced principal ideal which is closest to x. We write $\delta_1(x) = \delta(\mathfrak{a}(x), x)$. The notation $\hat{\mathfrak{a}}(x)$ will be used for the ideal computed by our procedure. We also use $\delta_2(x)$ to represent $\delta(\hat{\mathfrak{a}}(x), x)$ and $\hat{\delta}_1(x) = \hat{\delta}(\mathfrak{a}(x), x)$, $\hat{\delta}_2(x) = \hat{\delta}(\hat{\mathfrak{a}}(x), x)$ to denote the approximations we obtain to $\hat{\delta}_1(x)$ (if $\mathfrak{a}(x)$ is actually computed in our algorithm) and $\hat{\delta}_2(x)$ respectively.

The protocol can roughly be described as follows: The communication partners are A and B. A secretely chooses $a \in \{1, 2, \ldots, \lfloor\sqrt{D}\rfloor\}$ and B secretely chooses $b \in \{1, 2, \ldots, \lfloor\sqrt{D}\rfloor\}$. A computes $\hat{\mathfrak{a}}(a)$, $\hat{\delta}(a)$ and transmits the result to B. B determines $\hat{\mathfrak{a}}(b)$, $\hat{\delta}(b)$ and sends the result to A. From this information both partners are able to calculate $\hat{\mathfrak{a}}(ab)$. Although, this ideal is not neccessarily the same for A and B since the computational error might slightly differ with the different computing methods

of A and B, a little additional work will allow A and B to agree on a common ideal which is the secret key.

We will denote the roundoff errors by

$$\begin{aligned} \epsilon(\mathbf{a}, x) &= |\delta(\mathbf{a}, x) - \hat{\delta}(\mathbf{a}, x)|, \\ \epsilon_i(x) &= |\delta_i(x) - \hat{\delta}_i(x)|. \end{aligned}$$

3 Procedures

In the calculations, a basic precision constant δ_0 is used which will be specified later.

In order to calculate the secret key the communication partners use the following procedures which are described in Williams/Wunderlich [12]:

Procedure 1 *1.* **Input:** $\mathbf{a}, \mathbf{b} \in \mathcal{R}$, $\hat{\delta}(\mathbf{a}, x)$, $\hat{\delta}(\mathbf{b}, y)$ *for some* $x, y \in R_{>0}$.

2. **Output:** $\mathbf{ab}$, $\hat{\delta}(\mathbf{ab}, x + y) = \hat{\delta}(\mathbf{a}, x) + \hat{\delta}(\mathbf{b}, y)$.

3. **Property:** $\epsilon(\mathbf{ab}, x + y) \leq \epsilon(\mathbf{a}, x) + \epsilon(\mathbf{b}, y)$.

The error estimate in the previous procedure holds if $\max\{|\delta(\mathbf{a}, x)|, |\delta(\mathbf{b}, y)|\} < R/4$ where R is the regulator of K. This inequality will always be satisfied in our protocol.

Procedure 2 *1.* **Input:** $\mathbf{a} \in \mathcal{P}$ *which is a product of two reduced ideals,* $\hat{\delta}(\mathbf{a}, x)$ *for some* $x \in R_{>0}$.

2. **Output:** $\mathbf{b} \in \mathcal{R}$, $\hat{\delta}(\mathbf{b}, x)$.

3. **Property:** $|\hat{\delta}(\mathbf{b}, x) - \hat{\delta}(\mathbf{a}, x)| \leq \log(2D) + \delta_0$, $\epsilon(\mathbf{b}, x) \leq \epsilon(\mathbf{a}, x) + \delta_0$.

Procedure 3 *1.* **Input:** $\mathbf{a} \in \mathcal{R}$, $\hat{\delta}(\mathbf{a}, x)$ *for some* $x \in R_{>0}$.

2. **Output:** *The right neighbor* $N_+(\mathbf{a})$ *or the left neighbor* $N_-(\mathbf{a})$ *of* $\mathbf{a}$ *in the sequence* $(\mathbf{a}_j)$ *of reduced principal ideals and* $\hat{\delta}(N_+(\mathbf{a}), x)$ *or* $\hat{\delta}(N_-(\mathbf{a}), x)$.

3. **Property:** $\epsilon(N_\pm(\mathbf{a}), x) \leq \epsilon(\mathbf{a}, x) + \delta_0$.

If δ_0^{-1} and x and y are bounded by polynomials in D then the running time of all those procedures is a polynomial in $\log D$. The procedures are used in

Procedure 4 *1.* **Input:** $\hat{\mathbf{a}}(x)$, $\hat{\mathbf{a}}(y)$, $\hat{\delta}(x)$, $\hat{\delta}(y)$ *for some* $x, y \in R_{>0}$.

2. **Output:** $\hat{\mathbf{a}}(x + y)$, *the ideal that minimizes* $\hat{\delta}(\mathbf{a}, x + y)$ *over all* $\mathbf{a}$ *which are determined in this procedure. The ideal* $\mathbf{a}(x + y)$ *will be among those ideals although* $\hat{\delta}_1(x + y) > \hat{\delta}_2(x + y)$ *is possible and therefore* $\mathbf{a}(x + y)$ *might not be recognized.* $\hat{\delta}_2(x + y)$ *is also output.*

3. **Property**: *If* $\hat{\mathbf{a}}(x) \in \{\mathbf{a}_-(x), \mathbf{a}_+(x)\}$ *and* $\hat{\mathbf{a}}(y) \in \{\mathbf{a}_-(y), \mathbf{a}_+(y)\}$, *then* $\epsilon(\mathbf{a}, x+y) \leq (\epsilon_2(x) + \epsilon_2(y))C_1 + C_2$ *for every* $\mathbf{a}$ *determined in the procedure where* $C_1 = (1 + 4\delta_0/\kappa_3)$ *and* $C_2 = \delta_0(20\kappa_2 + 5\kappa_3 + 4\delta_0)/\kappa_3$ *and with* κ_2 *and* κ_3 *from (2) and (3) below.*

In order to describe Procedure 4 and to prove the above property we need the following inequalities which can also proved by using results of Williams [11]:

$$\kappa_1 = \frac{1}{1+\sqrt{D}} < \delta(N_+(\mathbf{a}), \mathbf{a}), -\delta(N_-(\mathbf{a}), \mathbf{a}) < \log\sqrt{D} = \kappa_2, \tag{2}$$

$$\delta(N_+^2(\mathbf{a}), \mathbf{a}), -\delta(N_-^2(\mathbf{a}), \mathbf{a}) > \log 2 = \kappa_3, \tag{3}$$

for every $\mathbf{a} \in \mathcal{R}$. Here we have used the notation $\delta(\mathbf{a}, \mathbf{b}) = \log\alpha$ for $\mathbf{a}, \mathbf{b} \in \mathcal{P}$ where $\alpha \in K_{\geq 1}$ is such that $\mathbf{b} = \frac{1}{\alpha}\mathbf{a}$ and $|\log\alpha|$ is minimal. Analogously, we will write $\hat{\delta}(\mathbf{a}, \mathbf{b})$ for the corresponding approximate value.

In Procedure 4 we first apply Procedure 1 to determine $\mathbf{c} = \hat{\mathbf{a}}(x)\hat{\mathbf{a}}(y)$ and $\hat{\delta} = \hat{\delta}(\mathbf{c}, x+y) = \hat{\delta}(x) + \hat{\delta}(y)$. Since $\delta(\mathbf{c}, x+y) = \delta_2(x) + \delta_2(y)$, we have

$$|\delta(\mathbf{c}, x+y) - \hat{\delta}| \leq \epsilon_2(x) + \epsilon_2(y)$$

Next, we apply Procedure 2 to obtain $\mathbf{b}$ and $\hat{\delta}(\mathbf{b}, x+y)$. We then have

$$|\delta(\mathbf{b}, x+y) - \hat{\delta}(\mathbf{b}, x+y)| < \epsilon_2(x) + e_2(y) + \delta_0.$$

In the sequel we assume that

$$\delta_0 \leq \kappa_3/4.$$

This guarantees by (3) that two consecutive applications of N_+ increase $\hat{\delta}$ at least by $\kappa_3/2$ and, analogously, that two consecutive applications of N_- decrease $\hat{\delta}$ at least by $\kappa_3/2$. Apply N_+ or N_- n times to $\mathbf{b}$ to obtain $\mathbf{b}'$ such that $|\hat{\delta}(\mathbf{b}', x+y)|$ is minimal. Put $\hat{\mathbf{a}}(x+y) = \mathbf{b}'$.

If $\hat{\mathbf{a}}(x) \in \{\mathbf{a}_-(x), \mathbf{a}_+(x)\}$ then

$$|\delta_2(x)| < |\delta_1(x)| + \kappa_2 < 3\kappa_2/2.$$

It follows that

$$|\delta(\mathbf{b}, x+y)| < 3\kappa_2 + \log(2D) = 5\kappa_2 + \kappa_3$$

and

$$|\hat{\delta}(\mathbf{b}, x+y)| < \epsilon_2(x) + \epsilon_2(y) + 5\kappa_2 + \kappa_3 + \delta_0.$$

Hence no more than $4(\epsilon_2(x) + \epsilon_2(y) + 5\kappa_2 + \kappa_3 + \delta_0)/\kappa_3$ applications of Procedure 3 are required to find $\hat{\mathbf{a}}(x+y)$ and $\hat{\delta}(x+y)$. Moreover, the error is bounded as asserted in Procedure 4.

Using Procedure 4 we are able to explain the basic algorithm used in the protocol which is based on the well known fast exponentiation technique.

Procedure 5 *1.* **Input:** $\hat{\mathbf{a}}(x)$, $\hat{\delta}(x)$, *for some* $x \in \mathcal{R}_{>0}$, $y \in \mathcal{Z}_{>0}$.

2. **Output:** $\hat{\mathbf{a}}(xy)$, $\hat{\delta}(xy)$.

3. **Algorithm**

(a) Determine the binary decomposition

$$y = \sum_{i=0}^{L} b_i 2^{L-i}, \qquad b_i \in \{0,1\}.$$

Set $z = 1$, $\hat{\mathbf{a}}(z) = \hat{\mathbf{a}}(x)$.

(b) For $1 \leq i \leq L$ *do:*

i. Compute $\hat{\mathbf{a}}(2z)$, $\hat{\delta}(2z)$ *by Procedure 4. Replace* $\hat{\mathbf{a}}(z)$, $\hat{\delta}(z)$ *by* $\hat{\mathbf{a}}(2z)$ *and* $\hat{\delta}(2z)$ *respectively.*

ii. If $b_i = 1$, *use Procedure 4 to compute* $\hat{\mathbf{a}}(z+x)$, $\hat{\delta}(z+x)$. *Replace* $\hat{\mathbf{a}}(z)$ *by* $\hat{\mathbf{a}}(z+x)$ *and* $\hat{\delta}(z)$ *by* $\hat{\delta}(z+x)$.

(c) Set $\hat{\mathbf{a}}(xy) = \hat{\mathbf{a}}(z)$, $\hat{\delta}(xy) = \hat{\delta}(z)$.

4 The protocol

We must now discuss how the communication partners can calculate the common secret key. We first require

Proposition 1 *Let* $x, y \in \mathcal{R}_{>0}$. *Assume that for the input of Procedure 4 we have* $\hat{\mathbf{a}}(x) \in \{\mathbf{a}_-(x), \mathbf{a}_+(x)\}$, $\hat{\mathbf{a}}(y) \in \{\mathbf{a}_-(y), \mathbf{a}_+(y)\}$, *and* $E = C_1(\epsilon_1(x)+\epsilon_2(x))+C_2 < \kappa_1/2$. *Then the ideal* $\hat{\mathbf{a}}(x+y)$, *determined by that Procedure, is either* $\mathbf{a}_-(x+y)$ *or* $\mathbf{a}_+(x+y)$.

Proof: It follows from the assumption and from the property of Procedure 4 that

$$|\hat{\delta}_2(x+y)| - |\hat{\delta}_1(x+y)| \geq |\delta_2(x+y)| - |\delta_1(x+y)| - 2E.$$

If $\hat{\mathbf{a}}(x+y) \notin \{\mathbf{a}_-(x+y), \mathbf{a}_+(x+y)\}$, then by (2) we have

$$|\hat{\delta}_2(x+y)| - |\hat{\delta}_1(x+y)| > \kappa_1 - 2E > 0$$

which contradicts the definition of $\hat{\mathbf{a}}(x+y)$. □

We must now develop a condition under which Procedure 5 will find an ideal $\hat{\mathbf{a}}(xy) \in \{\mathbf{a}_+(xy), \mathbf{a}_-(xy)\}$. We put $E_0 = \epsilon_2(x)$ and define

$$\begin{aligned} E'_{i+1} &= 2E_i C_1 + C_2 \\ E_{i+1} &= \begin{cases} E'_{i+1} & \text{when } b_{i+1} = 0 \\ (E'_{i+1} + E_0)C_1 + C_2) & \text{when } b_{i+1} = 1 \end{cases} . \end{aligned}$$

If at the ith iteration of Procedure 5 we have $\hat{\mathbf{a}}(z) \in \{\mathbf{a}_-(z), \mathbf{a}_+(z)\}$ then at the $i+1$-st iteration we have $\epsilon_2(z) < E_{i+1}$ and $\hat{\mathbf{a}}(z) \in \{\mathbf{a}_-(z), \mathbf{a}_+(z)\}$ when $E_{i+1} < \kappa_1/2$ by Proposition 1. If we put $M_0 = E_0$ and define

$$M_{i+1} = C_3 M_i + C_4$$

where $C_3 = 2C_1^2$, $C_4 = C_1C_2 + E_0C_1 + C_2$, then $E_i \leq M_L$ for $0 \leq i \leq L$. Thus,

$$\hat{\mathbf{a}}(xy) \in \{\mathbf{a}_-(xy), \mathbf{a}_+(xy)\}$$

when $M_L < \kappa_1/2$. Since

$$M_L = C_3^L M_0 + C_4(C_3^L - 1)/(C_3 - 1)$$

and

$$C_3^L < ey$$

for $\delta_0 < \kappa_3/(8L)$, we get

$$M_L < ey(E_0 + C_4).$$

Hence,

$$\epsilon_2(xy) < ey(E_0 + C_4). \tag{4}$$

We now calculate $\hat{\mathbf{a}}(1)$ and $\hat{\delta}_2(1)$ such that $\epsilon_2(1) < \delta_0$. Clearly, such values can be determined by the use of Procedure 3 and they are made public. Procedure 5 can then be used to determine $\hat{\mathbf{a}}(a)$, $\hat{\mathbf{a}}(b)$, $\hat{\delta}(a)$, $\hat{\delta}(b)$ and for the calculation of the value of $\hat{\mathbf{a}}(ab)$.

If δ_0^{-1} is polynomially bounded in D then this computation requires only polynomial time in $\log D$. From the error estimate (4) above, we see that

$$\epsilon_2(ab) = O(\delta_0 D \log D).$$

Thus both communaction partners A and B can compute one of two possible ideals in polynomial time in $\log D$.

Now consider one of the communication partners A or B and denote his ideal $\hat{\mathbf{a}}(ab)$ by $\hat{\mathbf{a}}$, Also write $\hat{\delta} = \hat{\delta}_2(ab)$, $\epsilon = \epsilon_2(ab)$, and $x = ab$. In order to develop a little additional protocol which makes the choice unique we need

Proposition 2 *Let $\epsilon < \kappa_1/8$. If $|\delta_1(x)| > \kappa_1/4$ then both communication partners can find out whether $\hat{\mathbf{a}} = \mathbf{a}_+(x)$ or $\hat{\mathbf{a}} = \mathbf{a}_-(x)$ and they can therefore both find $\mathbf{a}_+(x)$. If $|\delta_1(x)| < \kappa_1/4$ then they can both find $\mathbf{a}(x)$.*

Proof: It can be decided whether $\hat{\mathbf{a}}$ is on the left or on the right of x if $|\hat{\delta}| > \epsilon$. If $|\delta_1(x)| > \kappa_1/4$ then it follows from the minimality of $\delta_1(x)$ and from the choice of ϵ that $|\hat{\delta}| > \kappa_1/4 - \epsilon > \epsilon$.

On the other hand, both communication partners know that $\mathbf{a}(x) \in S = \{N_{\pm}(\hat{\mathbf{a}}), \hat{\mathbf{a}}\}$. If $|\delta_1(x)| < \kappa_1/4$ then S contains an ideal $\mathbf{b}$ with $|\hat{\delta}(\mathbf{b}, x)| < 3\kappa_1/8$ and thus both partners can deduce that $|\delta(\mathbf{b}, x)| < \kappa_1/2$ which by (2) means that $\mathbf{b} = \mathbf{a}(x)$. □

We can now formally describe the protocol:

Protocol 1 *1. A and B agree publically on D on $\hat{\mathbf{a}}(1)$ and on $\hat{\delta}(1)$ with $\epsilon(1) < \delta_0$ where δ_0 is chosen sufficiently small that the errors never exceed $\kappa_1/8$.*

2. A secretely chooses $a \in \{1, \ldots, \lfloor\sqrt{D}\rfloor\}$. A uses Procedure 5 to compute $\hat{\mathbf{a}}(a)$ and $\hat{\delta}(a)$. Both are sent to B.

3. B secretely chooses $b \in \{1, \ldots, \lfloor\sqrt{D}\rfloor\}$. B uses Procedure 5 to compute $\hat{\mathbf{a}}(b)$ and $\hat{\delta}(b)$. Both are sent to A.

4. From $\hat{\mathbf{a}}(a), \hat{\delta}(a)$ and b, B calculates $S_B = \{\hat{\mathbf{a}}(ab), N_{\pm}(\hat{\mathbf{a}}(ab))\}$. If possible, B computes $\mathbf{a}(ab)$ and sends '0' to A. Otherwise, B determines $\mathbf{a}_+(ab)$ and sends '1' to A.

5. From $\hat{\mathbf{a}}(b), \hat{\delta}(b)$ and a, A calculates $S_A = \{\hat{\mathbf{a}}(ab), N_{\pm}(\hat{\mathbf{a}}(ab))\}$. If A has received '0' from B, then A attempts to calculate $\mathbf{a}(x)$ and in case of success he sends '0' back to B. The secret key is $\mathbf{a}(x)$. Otherwise, A determines $\mathbf{a}_+(x)$ and sends '1' to B. If A has received '1' from B, then A attempts to calculate $\mathbf{a}_+(x)$ and in case of success he sends '1' back to B. The secret key is $\mathbf{a}_+(x)$. Otherwise, A determines $\mathbf{a}(x)$ and sends '1' to A.

6. If B has sent '0' and receives '1' then B determines the secret key $\mathbf{a}_+(x)$ which is possible by Proposition 2. If B has sent '1' and receives '0' then B determines the secret key $\mathbf{a}(x)$ which is possible by Proposition 2. Otherwise, the ideal determined initially by B is the secret key.

5 Security

In order to guarantee the security of our scheme it is neccessary that the number p of reduced principal ideals of $\mathcal{O}$ be sufficiently large. From Williams [11] we know the following lower bound :

$$p \geq \frac{1}{\log D} R$$

where R is the regulator of $\mathcal{O}$. Moreover, as noted by Shanks [10], it follows from a result of Littlewood (see also Mollin/Williams [7]) that

$$hR >> D^{1/2-\epsilon}$$

for arbitrarily small ϵ where h is the class number of $\mathcal{O}$. To make p large we must therefore find and use real quadratic orders with small class numbers. For certain choices of D the even part of h can easily be bounded, e.g. if D is a prime number, 8 times a prime number, or the product of two prime numbers which are both congruent to 3 mod 4 then h is odd (see Kaplan [4]). On the other hand, it follows from the conjectural statements of Cohen/Lenstra [2] that the probability for the odd part of the class number to be bounded by $\log D$ is $1 - o(1)$ for $D \to \infty$.

We can therefore expect that if we choose the right discriminants then the probability that $p >> D^{1/2-\epsilon}$ is $1 - o(1)$ for arbitrarily small ϵ and $D \to \infty$.

We must now discuss the difficulty of breaking the scheme. We conjecture that being able to break the scheme implies being able to factor. So far we can only prove the following: Consider the *discrete logarithm problem* for reduced ideals of real quadratic orders (DLP): for any given reduced ideal $\mathfrak{a}$ compute $\delta(\mathfrak{a}, \mathcal{O})$.

Proposition 3 *If DLP can be solved in polynomial time then the key exchange protocol can be broken in polynomial time.*

Proof: Knowing $\hat{\mathfrak{a}}(a)$ and $\hat{\delta}(a)$ the enemy can use the algorithm for solving DLP to come up with $x, y \in R$ such that $\hat{\mathfrak{a}}(a) = \hat{\mathfrak{a}}(x)$. Knowing $x, \hat{\mathfrak{a}}(b), \hat{\delta}(b)$ he can then use Procedure 5 to calculate the secret key. □

Proposition 4 *If there is a polynomial time solution of DLP then one can factor in polynomial time.*

Proof: We show that a polynomial time solution of DLP can be used to determine the regulator R of $\mathcal{O}$ in polynomial time. One can then use the method described in Schoof [8] to factor in polynomial time.

In order to find the regulator, we start with the second reduced ideal $\mathfrak{a}_2$. Its distance from $\mathcal{O}$ is by (3) at least $\log 2$. By repeatedly squaring and reducing this ideal we obtain a sequence of reduced ideals whose distances from $\mathcal{O}$ will be first increasing exponentially. Since those distances are bounded by R we find in polynomial time a reduced ideal whose distance is less than the distance of the previous ideal in the sequence. By applying a "divide and conquer" method, the regulator can be found in polynomial time. □

References

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

[2] H. Cohen and H.W. Lenstra Jr., *Heuristics on class groups of number fields*, Number Theory (Nordwijkerhout, 1983), Lecture Notes in Math. **1068**, 33–62, Springer Verlag Berlin and New York, 1984.

[3] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory **22** (1976), 472–492.

[4] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. **283/284** (1976), 313–363.

[5] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), 203–209.

[6] K.S. McCurley, *A key distribution system equivalent to factoring*, J. Cryptology **1** (1988), 95–105.

[7] R.A. Mollin and H.C. Williams, *Computation of the class number of a real quadratic field*, preprint (1988).

[8] R.J. Schoof, *Quadratic fields and factorization* in *Computational methods in number theory*, H.W. Lenstra Jr. and R. Tijdeman, eds. , Math. Centrum Tracts **155**, Part II, Amsterdam (1983), 235–286.

[9] D. Shanks, *The infrastructure of a real quadratic field and its applications*, Proc. 1972 Number Theory Conf., Boulder, Colorado, (1973), 217–224.

[10] D. Shanks, *Systematic examination of Littlewood's bounds on* $L(1, \chi)$, Proc. Sympos. Pure Math. **24**, AMS Providence RI (1973), 267–283.

[11] H.C. Williams, *Continued fractions and number-theoretic computations*, Rocky Mountain J. Math. **15** (1985), 621–655.

[12] H.C. Williams and M.C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*, Math. Comp. **48** (1987), 405–423.