Cryptographic Protocols Based on Discrete Logarithms in Real-quadratic Orders

Ingrid Biehl Johannes Buchmann Christoph Thiel

Fachbereich Informatik
Universität des Saarlandes
Postfach 151150, 66041 Saarbrücken, Germany

Abstract. We generalize and improve the schemes of [4]. We introduce analogues of exponentiation and discrete logarithms in the principle cycle of real quadratic orders. This enables us to implement many cryptographic protocols based on discrete logarithms, e.g. a variant of the signature scheme of ElGamal [8].

1 Introduction

1.1 Motivation

The security of many cryptographic protocols (see for example [7], [8], [12]) is based on the difficulty of solving the *discrete logarithm problem* (DL-problem) in the multiplicative group $GF(p)^*$ of prime fields $GF(p)$ of characteristic $p > 0$.

Recently, Gordon [9] has shown that under reasonable assumptions the discrete DL-problem in GF$(p)^*$ can be solved in expected time

$$L_p[1/3, c] = exp((c + o(1)) \cdot (\log p)^{1/3} \cdot (\log \log p)^{2/3})$$

by means of the number field sieve (NFS), thereby lowering the best known asymptotically upper bound considerably. Experience with similar integer factoring algorithms shows that the NFS can be expected to be practical (see [5], [1]). It is therefore by no means clear that the discrete logarithm problem remains difficult in the future and one must search for other problems that can serve as basis for one-way and trapdoor one-way functions (see for example [4], [10], [11]). It would be useful to have some sort of hierarchy of difficult problems. If one of the problems turns out to be easy one can use the next difficult one that remains intractable. A first step in this direction is to employ algebraic number fields (see [3]) as a source for computationally hard problems. In [4], [13] it is shown how to use the infrastructure of the cycles of reduced ideals in real quadratic orders to implement the Diffie-Hellman key exchange protocol. Breaking that scheme was shown to be at least as hard as factoring. Also, it was the first case of a Diffie-Hellman-implementation which is not based on the arithmetic of a finite abelian group. That application, however, looks rather restricted since it only solves the problem of key management. In this paper we

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 56-60, 1994.

generalize and improve the scheme of [4]. We introduce analogoues of exponentiation and discrete logarithms in the principle cycle of real quadratic orders. This enables us to implement many cryptographic protocols which are based on discrete logarithms, e.g. the ElGamal scheme [8], and we argue that computing generalized discrete logarithms is at least as hard as factoring.

1.2 Discrete Logarithms in Real-quadratic Orders

Let $\mathcal{D}$ be the set of all $\Delta \in \mathbb{Z}_{>0}$ which are no squares in $\mathbb{Z}$ and satisfy $\Delta \equiv 0, 1 \bmod 4$. Let $\Delta \in \mathcal{D}$. Then $\mathcal{O}_\Delta = \mathbb{Z} + \frac{\Delta+\sqrt{\Delta}}{2}\mathbb{Z}$ is the *real quadratic order of discriminant* Δ. The *field of fractions* of $\mathcal{O}_\Delta$ is $\mathrm{K}_\Delta = \mathbb{Q}(\sqrt{\Delta})$, its multiplicative group is denoted by K_Δ^*. For $\alpha \in \mathrm{K}_\Delta$, $\alpha = (x + y\sqrt{\Delta})/(2z)$ with $x, y, z \in \mathbb{Z}$, $z > 0$ and $\gcd(x, y, z) = 1$, we set $\overline{\alpha} = (x - y\sqrt{\Delta})/(2z)$.

A finitely generated $\mathcal{O}_\Delta$-module $A \subseteq \mathrm{K}_\Delta$, $A \neq \{0\}$ is called *fractional ideal* of $\mathcal{O}_\Delta$. It can be written as $A = q\left(\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}\right)$, where $a, b \in \mathbb{Z}, q \in \mathbb{Q}$, $a, q > 0$, and $c = (b^2 - \Delta)/(4a) \in \mathbb{Z}$. The numbers a and q are uniquely determined whereas b is unique modulo $2a$. To make the representation unique we choose $-2a + \sqrt{\Delta} < b < \sqrt{\Delta}$ if $a < \sqrt{\Delta}$, and $-a < b \leq a$ if $a > \sqrt{\Delta}$. If $q = 1$ then A is called *normal* . We will only use normal ideals and write $a = a(A)$, $b = b(A)$, $c = c(A)$. We also define $\gamma(A) = \frac{b+\sqrt{\Delta}}{2a}$, so $A = \mathbb{Z} + \gamma(A)\mathbb{Z}$. Fractional ideals A, B of $\mathcal{O}_\Delta$ are called *equivalent* if there is $\alpha \in \mathrm{K}_\Delta^*$ such that $A = \alpha B$. The number α is called *generator of A relative to B*. If $B = \mathcal{O}_\Delta$ then A is called *principle* and α is called *generator* of A. The equivalence classes of the above equivalence relation are called *ideal classes*.

In cryptosystems based on real quadratic orders, the analogue of the finite field $\mathrm{GF}(p)$ is the set of reduced principal ideals. An ideal A of $\mathcal{O}_\Delta$ is called *reduced* if $\gamma(A) > 1$ and $-1 < \overline{\gamma(A)} < 0$. If A is reduced, then $a(A), |b(A)| < \sqrt{\Delta}$. Thus, the set $\mathcal{R}_\Delta$ of reduced principle ideals of $\mathcal{O}_\Delta$ is finite.

Shanks [14] discovered that $\mathcal{R}_\Delta$ resembles a cyclic group. This enables us to formulate a discrete logarithm problem in $\mathcal{R}_\Delta$. If A, B are ideals of $\mathcal{O}_\Delta$, α a generator of A relative to B then the set of all generators of A relative to B is $\{\eta\alpha : \eta \text{ is a unit of } \mathcal{O}_\Delta\}$. There is a unique unit ϵ in $\mathcal{O}_\Delta$ with $\epsilon > 1$ such that any other unit η in $\mathcal{O}_\Delta$ can be written as $\eta = \pm\epsilon^k$ with $k \in \mathbb{Z}$. Hence the generators of A relative to B are of the form $\alpha' = \pm\epsilon^k\alpha$, $k \in \mathbb{Z}$, and we have $\log|\alpha'| = \log|\alpha| + k\mathrm{R}_\Delta$ where $\mathrm{R}_\Delta = \log\epsilon$ is the *regulator* of $\mathcal{O}_\Delta$. The residue class $\log|\alpha| + \mathrm{R}_\Delta\mathbb{Z}$ is called *distance* from A to B. That distance is denoted by $\delta(A, B)$. If $A = \mathcal{O}_\Delta$ then we briefly write $\delta(B)$. On a circle of circumpherence R_Δ fix a point for $\mathcal{O}_\Delta$. Then $B \in \mathcal{R}_\Delta$ corresponds to a point on that circle whose distance from $\mathcal{O}_\Delta$ is $\delta(B)$. The set $\mathcal{R}_\Delta$ forms a cyclic graph. In that graph, each reduced principle ideal has a *left neighbor* and a *right neighbor*.

We explain exponentiation in $\mathcal{R}_\Delta$. We associate with $k \in \mathbb{R}$ a pair (A, c) consisting of the nearest reduced principal ideal A to k and the distance from k to A. That nearest ideal is defined by the property that there is $\alpha \in \mathcal{O}_\Delta$, with

$(1/\alpha)\mathcal{O}_\Delta = A$ and such that $|\log|\alpha| - k| < |\log|\alpha'| - k|$ for all $\alpha' \in \mathcal{O}_\Delta$. The distance from k to A is $c = \log|\alpha| - k$. In case that A is not uniquely determined by those conditions we make A unique by requiring c to be positive. Let m be a positive integer. Let $A \in \mathcal{R}_\Delta$ and c a real number. Let $\delta \in \delta(A)$. The mth power of (A, c) is a pair (B, d) where B is the reduced principal ideal which is nearest to $x = m(\delta + c)$ and d is the distance from x to B. This power is independent of the choice of δ and is denoted by $\exp((A, c), m)$. It is easy to see that if $A \in \mathcal{R}_\Delta$, $c \in \mathbb{R}$, $k, m \in \mathbb{Z}_{>0}$ then we have $\exp(\exp((A, c), k), m) = \exp(\exp((A, c), m), k)$. This statement enables us to implement many cryptographic protocols. The difficulty of inverting exp follows from the following theorem which can be proved using ideas similar to those explained in [4].

Theorem 1. *There is a probabilistic polynomial time reduction of factoring integers to inverting* exp.

2 Computing Powers

Let c be a complex number, and let $q \in \mathbb{Z}_{>0}$. An *approximation of precision* q to c is a number $\hat{c} \in 2^{-(q+1)}\mathbb{Z}[i]$ such that $|c - \hat{c}| < 2^{-q}$.

We now present the algorithm EXP. Let $A \in \mathcal{R}_\Delta$, $c \in \mathbb{Q}$, $x \in \mathbb{Z}_{>0}$, $\delta \in \delta(A)$, and $\exp((A, c), x) = (B, d)$. Given A, c, x, and a sufficiently large precision $p \in \mathbb{Z}_{>0}$ EXP determines B or its left neighbor and an approximation d of precision p to the distance between B and $x(d + c)$. Since there might be two ideals in $\mathcal{R}_\Delta$ of almost equal distance from $x(\delta + c)$, it is, in general, not clear, whether B itself can be computed in polynomial time.

Algorithm 2 (EXP).

Input: $\Delta \in \mathcal{D}$, $p \in \mathbb{Z}$, $p \geq \lceil 3 + \log \Delta \rceil$, $A \in \mathcal{R}_\Delta$, $c \in \mathbb{Q}$, $x \in [0, \ldots, \lceil\sqrt{\Delta}\rceil]$.
Output: *As specified above*

$C := \mathcal{O}_\Delta$; $p' := p + 3 \cdot \lceil \log \Delta \rceil + 3$		(1)
IF $x = 1$		(2)
THEN	$\xi := 1$; $C := A$; $m := 0$; $\ell := c$	(3)
ELSE	*Compute the binary decomposition* $x = \sum_{i=0}^{m} x_i 2^i$ *with* $m = \lceil \log x \rceil$, $x_i \in \{0, 1\}$ *for* $0 \leq i \leq m$; $d = 0$; $\ell := 0$	(4)
	FOR $i = 0, 1, \ldots, m$	(5)
	$\gamma_i := 1$	(6)
	IF $x_i = 1$ *THEN* $C := CA$; $\ell := \ell + d$	(7)
	$(A, \gamma_i) := REDUCE(\Delta, (A)^2)$; $d := 2d + APPROX(\Delta, \gamma_i, p')$	(8)
	$(C, \gamma) := REDUCE(\Delta, C)$; $\ell := -\ell + cx - APPROX(\Delta, \gamma, p')$	(9)
$\alpha := TARGET(\Delta, C, \ell)$		(10)
$B := (1/\alpha)C$; $d := \ell - APPROX(\Delta, \alpha, p')$		(11)

EXP determines its result by means of binary exponentiation. The basic operation in the set of reduced principal ideals is ideal multiplication which can be performed in quadratic time followed by ideal reduction which also requires quadratic time. Reduction of ideals is performed using the procedure REDUCE which on input of the discriminant Δ and an ideal B of $\mathcal{O}_\Delta$ returns a reduced ideal in the ideal class of B and a generator γ of B relative to C. If we compute a reduced principal ideal C in the class of the product of two reduced principal ideals B and B' using REDUCE then $\delta(C) = \delta(B) + \delta(B') + \log|\gamma|$. While carrying out binary exponentiation in EXP we therefore accumulate the error term $\log|\gamma|$ in the variable ℓ. This is done using APPROX which given Δ, a number γ in K_Δ and a precison constant q finds in linear time an approximation of precison q to $\log|\gamma|$. After executing the FOR loop we have found an ideal C which is close to $x\delta + \ell$. Procedure TARGET then determines a generator of C relative to the real output ideal B. TARGET uses the procedures which were introduced in [6]. Its correctness follows from the arguments presented there. We will show in the full paper that the running time of EXP is cubic just as exponentiation in GF(p).

Algorithm 3 (TARGET).

Input: $\Delta \in \mathcal{D}$, *a reduced principal ideal* A *of* $\mathcal{O}_\Delta$, $s \in \mathbb{Q}_{>0}$.
Output: *A minimum* α *that is closest to* s *or the left neighbor of it.*

$p := \lceil 3 + \log \Delta \rceil$	*(1)*
$\xi := CLOSE(\Delta, A, s)$; $e := s - APPROX(\Delta, \xi, p)$	*(2)*
$\eta := NEAREST(\Delta, (1/\xi) \cdot B, e, p)$; $\alpha := \xi \cdot \eta$; $r := APPROX(\Delta, \alpha, p) - s$	*(3)*
IF $r \geq 0$ *THEN* $\alpha := LMIN(\Delta, B, \alpha)$	*(4)*

2.1 Cryptographic Applications of EXP

We need another simple but important procedure MULT which replaces the multiplication in GF(p). Let A, B be reduced principal ideals, $a, b \in \mathbb{Q}$, and let I be the reduced principal ideal such that $\delta(I)$ is as close as possible to $\delta(A)+\delta(B)+a+b$. Given (A, a), (B, b) and a precision $p \in \mathbb{Z}_{>0}$ MULT determines a pair (C, c) where $C = I$ or C is the left neighbor of I and c is an approximation of precision p to the absolute smallest representative of $\delta(C)-\delta(A)-\delta(B)-a-b$. MULT can be easily implemented using the techniques of [6]. Details will be presented in the full paper.

Using MULT and EXP one can implement many cryptographic protocols. Clearly, the Diffie-Hellman key exchange protocol can be implemented using those techniques. Here we present a variant of the ElGamal sigature scheme [8]. Suppose that Alice wants to be able to sign messages. She chooses a real quadratic discriminant Δ and a reduced principal ideal A of $\mathcal{O}_\Delta$ for which she knows a good approximation a of a representative of $\delta(A)$. That can be realised by randomly choosing a number $a' \in \mathbb{R}$ and by a procedure CLOSEIDEAL which given a' and a precision p computes in polynomial time A and a such that

A is an ideal closest to a' or its left neighbor and a is an approzimation of some $\delta \in \delta(A)$ of precision p. Both Δ and A are made public. Also, the precision in the following computation is $p = \lceil 3 + \log \Delta \rceil$.

To sign the message $m \in \mathbb{Z}$, $m \in \{1, 2, \ldots, \lfloor\sqrt{\Delta}\rfloor\}$ Alice randomly chooses $r \in \{1, 2, \ldots, \lfloor\sqrt{\Delta}\rfloor\}$ and determines $(X, x) = \mathrm{EXP}((\mathcal{O}_\Delta, 1), r, p)$. The distance of X is very close to r. The number x is the corresponding correction term. Next, Alice computes $b = (m - a)/r$, $b_1 = \lfloor b \rfloor$, $b_2 = b - b_1$. Also, she determines a reduced principal ideal C which is close to rb_2 and the corresponding correction term c. The signature is $((X, x), b_1, (C, c), m)$. In order for Bob to verify the signature he computes $(Y_1, y_1) = \mathrm{EXP}((X, x), b_1, p)$, $(Y_2, y_2) = \mathrm{MULT}((A, 0), (Y_1, y_1), p)$, $(Y_3, y_3) = \mathrm{MULT}((Y_2, y_2), (C, c), p)$. It is easy to see that Y_3 must be the reduced principal ideal which is closest to m or its left neighbor. If this is incorrect then the signature is incorrect. As in the original ElGamal scheme, there is currently no other way of breaking this scheme than inverting exp and finding r or a. Again, a formal version of this protocol will be presented in the full version.

References

1. Bernstein, D.J., Lenstra, A.K.: A general number field sieve implementation. In: A. K. Lenstra, H. W. Lenstra, Jr. (Eds.) The Development of the Number Field Sieve (LNM 1554) (1993), Springer-Verlag, pp. 103-126
2. Buchmann, J., Thiel, C., Williams, H.C.: Short representation of quadratic integers. To appear in Proc. of CANT 1992
3. Buchmann, J.: Number Theoretic Algorithms and Cryptology. Proc. of FCT'91 (LNCS 529) (1991), Springer-Verlag, pp.16-21
4. Buchmann, J., Williams, H.C.: A Key Exchange System Based on Real-quadratic Fields. Proc. of CRYPTO'89 (LNCS 435) (1989), Springer-Verlag, pp. 335-343
5. Buchmann, J., Loho, J., Zayer, J.: An Implementation of the General Number Field Sieve. Proc. of CRYPTO'93 (LNCS 773) (1993), Springer-Verlag, pp. 159-165
6. Biehl, I., Buchmann, J.: Algorithms for quadratic orders. To appear in Proc. of Symposia in Applied Mathematics (1993)
7. Diffie, W., Hellman, M.: New directions in Cryptography. IEEE Trans. Inform. Theory 22 (1976), pp. 472-492
8. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory 31 (1985), pp. 469-472
9. Gordon, D.: Discrete Logarithms in $GF(p)$ Using the Number Field Sieve. Siam Jour. on Discrete Math. 6 (1993), pp. 124-138
10. Koblitz, N.: Elliptic curve cryptosystems. Math. Comp. 48 (1987), pp. 203-209
11. Miller, V.: Use of Elliptic Curves in Cryptography. Proc. of CRYPTO'85 (LNCS 218) (1986), Springer-Verlag, pp. 417-426
12. National Institute of Standards and Technology. The Digital Signature Standard, proposal and discussion. Comm. of the ACM, 35 (7), Juli 1992, pp. 36-54
13. Scheidler, R., Buchmann, J., Williams, H.C.: Implementation of a Key Exchange Protocol Using Real Quadratic Fields. Proc. of EUROCRYPT'90 (LNCS 473) (1990), Springer-Verlag, pp. 98-109
14. Shanks, D.: The infrastructure of a real quadratic field and its applications. Proc. of the 1972 Number Theory Conference, Boulder (1972), pp. 217-224