An efficient solution of the congruence

Article *in* IEEE Transactions on Information Theory · September 1987

DOI: 10.1109/TIT.1987.1057350 · Source: dx.doi.org

2 authors, including:

Claus Peter Schnorr
Goethe-Universität Frankfurt am Main
172 PUBLICATIONS **10,676** CITATIONS

An Efficient Solution of the Congruence $x^2 + ky^2 = m \pmod n$

JOHN M. POLLARD AND CLAUS P. SCHNORR

Abstract—**The equation of the title arose in the proposed signature scheme of Ong–Schnorr–Shamir. The large integers n, k and m are given and we are asked to find any solution x, y. It was believed that this task was of similar difficulty to that of factoring the modulus n; we show that, on the contrary, a solution can easily be found if k and m are relatively prime to n. Under the assumption of the generalized Riemann hypothesis, a solution can be found by a probabilistic algorithm in $O(\log n)^2|\log\log|k||)$ arithmetical steps on $O(\log n)$-bit integers. The algorithm can be extended to solve the equation $X^2 + KY^2 = M \pmod n$ for quadratic integers K, $M \in \mathbb{Z}[\sqrt{d}]$ and to solve in integers the equation $x^3 + ky^3 + k^2z^3 - 3kxyz = m \pmod n$.**

I. Introduction

THE CONCEPT of *digital signature* was proposed by Diffie and Hellman [5], together with that of *public-key cryptosystem*. The Rivest–Shamir–Adleman (RSA) method [15] is generally considered best for both uses. Research by Ong, Schnorr, and Shamir [12] led to a new method for signatures which seemed to be much easier to implement. In the system [12], the public key consists of two integers n and k. The modulus n is a large odd composite number (say, 1000 bits), whose factorization is kept secret; k is in general of similar size to n. A valid signature of the message m, where $0 < m < n$, is any pair of integers x, y with

$$x^2 + ky^2 \equiv m \pmod n. \tag{1}$$

It has been shown that general solutions of (1) can easily be generated when a square root $u = \sqrt{-1/k} \pmod n$ is given as private key. For any integer r, with r relatively prime to n, put $x = (m/r + r)/2 \pmod n$ and $y = (m/r - r)u/2 \pmod n$. Unlike the RSA method, there are many possible signatures for any message.

We give a probabilistic algorithm to solve (1) without knowing the factorization of n, which terminates in $O((\log n)^2|\log\log|k||)$ arithmetical operations on $O(\log n)$-bit numbers provided that k and m are relatively prime to n. This time bound holds under the assumption of the generalized Riemann hypothesis. The algorithm breaks the Ong–Schnorr–Shamir signature scheme.

Manuscript received October 8, 1985; revised September 29, 1986.

J. M. Pollard resides at Tidmarsh Cottage, Manor Farm Lane, Tidmarsh, Reading, Berks RG8 8EX, England.

C. P. Schnorr is with Fachbereich Mathematik/Fachbereich Informatik, Universität Frankfurt, PSF 11 19 32, 6000 Frankfurt a. M., West Germany.

IEEE Log Number 8613566.

For a natural number n let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ be the ring of integers modulo n, and let $\mathbb{Z}_n^*$ be the multiplicative group of integers modulo n which are relatively prime to n. For an odd prime p and integer k let (k/p) be the Legendre symbol. For integers a, b the greatest common divisor of a, b is denoted (a, b).

For a prime power $n = p^e$ it is known that $x^2 + ky^2 = m \pmod{p^e}$ is solvable for all k, $m \in \mathbb{Z}_{p^e}^*$, and we can find a solution in random polynomial time (i.e. using some random bits we can find in polynomial time integers which solve the equation with probability at least $1/2$). The restriction that the integers k, m be relatively prime to p is necessary. For instance, $x^2 = m \pmod{p^e}$ is solvable iff m is a square mod p^e. Since the order of the group $\mathbb{Z}_{p^e}^*$ is $p^{e-1}(p-1)$, we can compute square roots modulo p^e in random polynomial time using a probabilistic version of well-known square root algorithms (see, e.g., Rabin [14], Adleman *et al.* [1]). Given a square $a \pmod{p^e}$, these algorithms find $\pm\sqrt{a} \pmod{p^e}$ with probability $\geq 1/2$ within $O(e \log p)$ arithmetical operations modulo p^e. To solve (1) we pick a random $y \in \mathbb{Z}_{p^e}$ and apply the square root algorithm to $a := m - ky^2 \pmod{p^e}$. With probability at least $1/2$, $a \pmod{p^e}$ is square, and yields a solution $x := \sqrt{a} \pmod{p^e}$, y.

Suppose the prime factors of $n = \prod_{i=1}^{r} p_i^{e_i}$ are known. By the Chinese remainder theorem, (1) is solvable iff there exist integers x_i, y_i with $x_i^2 + ky_i^2 = m \pmod{p_i^{e_i}}$ for $i = 1, \cdots, r$. Therefore, given the prime factors of n, (1) can be solved probabilistically in $O(\log n)$ arithmetical operations on $O(\log n)$-bit integers using the Chinese remainder construction and the square root algorithm.

We outline the solution of (1) in Section II and describe the main step along with some alternatives in Section III. Section IV deals with exceptional cases. The time analysis is given in Section V. Section VI gives a solution of (1) via lattice basis reduction. In Section VII we discuss connections with the theory of Legendre's equation. In Section VIII we reduce the problem of solving, in quadratic integers $X, Y \in \mathbb{Z}[\sqrt{d}]$, the equation $X^2 + KY^2 = M \pmod n$ to the problem of solving (1). In Section IX we outline a solution of the equation $x^3 + ky^3 + k^2z^3 - 3kxyz = m \pmod n$.

Some related work has been stimulated by an early circulating draft of the main algorithm. J. Shallit [16] gave an exposition of Pollard's algorithm along with a preliminary analysis. Estes *et al.* [6] independently of this paper

0018-9448/87/0900-0702$01.00

extended the algorithm to quadratic integers. They also announced a version of the algorithm that does not rely on the assumption of the generalized Riemann hypothesis [2].

II. Outline of Algorithm

The new algorithm for solving (1) does not require knowledge of the prime factors of n. It is based on the well-known identity

$$x_1^2 + ky_1^2\left(x_2^2 + ky_2^2\right) = X^2 + kY^2 \tag{2}$$

where

$$X = x_1x_2 \pm ky_1y_2, \qquad Y = x_1y_2 \mp x_2y_1, \tag{3}$$

and solves (1) for k, $m \in \mathbb{Z}_n^*$. It was mentioned in [12] that we can interchange k and m; changing to new variables $x' = x/y$, $y' = 1/y \pmod n$, we have $x'^2 - my'^2 = -k \pmod n$. Our additional idea is that m can be replaced by a smaller number m' without affecting the difficulty of solving (1). Then we have the following algorithm that solves (1) for k, $m \in \mathbb{Z}_n^*$.

1) If n is a pure prime power then solve (1) by computing square roots in $\mathbb{Z}_n^*$.
2) Replace m by an equivalent m' such that $0 < m' \le \sqrt{4k/3}$ in case $k > 0$, and $0 < |m'| \le \sqrt{|k|}$ in case $k < 0$.
3) If m' is a perfect square, or $m' = k$, solve $x^2 + ky^2 = m' \pmod n$ with $y = 0$ or $x = 0$, and go to step 5).
4) Apply the algorithm recursively to solve $x'^2 - m'y'^2 = -k \pmod n$ such that $(y', n) = 1$. Solve $x^2 + ky^2 = m' \pmod n$ with $x := x'/y'$, $y := 1/y' \pmod n$.
5) Work back to a solution of the original equation.

Steps 2) and 4) reduce (k, m) to $(-m', -k)$, which halves the number of bits of $|k|$. By $O(|\log\log|k||)$ reduction steps the original pair (k, m) can be reduced to one of the pairs $(1,1)$, $(-1,1)$, or $(-1,-1)$ (the pair $(1,-1)$ is reduced in step 2) to $(1,1)$) for which the equation is solved directly in step 3). The reduction may terminate in step 3) before reaching $(1,1)$ or $(-1,1)$ or $(-1,-1)$.

III. The Main Step

We explain step 2) in more detail. We show how to find m' such that

$$\begin{aligned} &0 < m' \le \sqrt{4k/3}, && \text{in case } k > 0 \\ &0 < |m'| \le \sqrt{|k|}, && \text{in case } k < 0, \end{aligned} \tag{4a}$$

and from a solution of

$$x^2 + ky^2 = m' \pmod n \tag{4b}$$

it is easy to obtain a solution of (1).

Our first goal is to transform m into a prime m_0 with $(-k/m_0) = 1$, and to solve $x_0^2 = -k \pmod{m_0}$. For this we repeatedly pick random $u, v \pmod n$ with $u^2 + kv^2 \in \mathbb{Z}_n^*$, form $m_0 := m(u^2 + kv^2) \pmod n$, and try to solve

$$x_0^2 = -k \pmod{m_0} \tag{5}$$

using a probabilistic square root algorithm that finds x_0 with probability $\ge 1/2$ provided m_0 is prime. If the generalized Riemann hypothesis (GRH) holds, we need to try at most $O(\log n)$ pairs u, v on average in order to find a prime m_0 and x_0. We do not certify primality of m_0 but verify (5) instead. When m_0, x_0, u, and v are known it remains to solve $x'^2 + ky'^2 = m_0 \pmod n$. Then x'', y'' can be combined with u, v via (2), (3) to give a solution x, y of (1) with right-hand side $m_0^2/m \pmod n$, and thus $x := x''m/m_0$, $y := y''m/m_0 \pmod n$ solves (1).

Next we define integers $m_1, x_1, m_2, x_2, \cdots, x_{I-1}, m_I = m'$ by

$$\begin{aligned} x_0^2 + k &= m_0m_1 \\ x_1 &= \min\left(x_0 \bmod m_1, m_1 - (x_0 \bmod m_1)\right) \\ &\vdots \\ x_i^2 + k &= m_im_{i+1} \\ x_{i+1} &= \min\left(x_i \bmod m_{i+1}, m_{i+1} - (x_i \bmod m_{i+1})\right) \\ &\vdots \\ x_{I-1}^2 + k &= m_{I-1}m_I. \end{aligned} \tag{6}$$

We continue this iteration until we reach $i = I$ with

$$\begin{aligned} &x_{I-1} \le m_I \le m_{I-1}, && \text{if } k > 0 \\ &|m_I| \le \sqrt{|k|}, && \text{if } k < 0. \end{aligned} \tag{7}$$

Eventually we obtain a number $m' = m_I$ with the required properties (4a), (4b). To see this we consider separately the cases $k > 0$ and $k < 0$. We assume that $(m_i, n) = 1$ for $i = 0, \cdots, I$ and discuss the case $(m_i, n) \ne 1$ in Section IV.

For property (4a): If $k > 0$, then the numbers $m_1, m_2, \cdots$ are all positive. The iteration (6) is the Gaussian algorithm for reducing the quadratic form

$$\begin{bmatrix} x \\ y \end{bmatrix}^T \begin{bmatrix} m_0, & x_0 \\ x_0, & m_1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = m_0x^2 + 2x_0xy + m_1y^2.$$

This algorithm yields an integer 2×2-matrix T with $\det T = 1$ so that

$$\begin{bmatrix} m_0, & x_0 \\ x_0, & m_1 \end{bmatrix} = T^T \begin{bmatrix} m_I, & x_{I-1} \\ x_{I-1}, & m_{I-1} \end{bmatrix} T$$

and $m_I \le \sqrt{4k/3}$; the latter follows easily from (6), (7). The iteration (6) takes no more than $O(\log|x_0|)$ steps (see Lagarias [7]).

If $k < 0$, then negative m_i are possible. If $m_i, m_{i+1} > 0$, then

$$m_{i+1} = \frac{1}{m_i}\left(x_i^2 - |k|\right) < \frac{1}{4}m_i.$$

Therefore there exists $j = O(\log n)$ such that $m_{j+1} \le 0$ for the first time. Suppose that $m_{j+1} < 0$ (see Section IV for the case $m_{j+1} = 0$). Now we have $|x_j|^2 < |k|$. So if $|m_j| > \sqrt{|k|}$, then

$$|m_{j+1}| \le |k|/|m_j| \le \sqrt{|k|}.$$

This shows $I \le j + 1$.

To demonstrate property (4b), we multiply the equations

$$x_i^2 + k = m_i m_{i+1}, \qquad \text{for } i = 0,1,\cdots,I-1$$

together, using the identity (2), (3). So we obtain integers s,t with

$$s^2 + kt^2 = m_0(m_1 m_2 \cdots m_{I-1})^2 m_I, \tag{8}$$

or writing $U = s/M$, $V = t/M$, $M = m_1 m_2 \cdots m_I (\mathrm{mod}\, n)$,

$$U^2 + kV^2 = m_0/m_I (\mathrm{mod}\, n). \tag{9}$$

This again requires that $(m_i, n) = 1$ for $i = 1,\cdots,I$.

Now if a solution of (4) was known, we could similarly multiply (4) and (9), and so solve (1). This multiplication will be part of step 4); we conclude step 2) by storing the values of U and V.

Remarks

a) The recursion (6) was suggested by the proof of Fermat's two-square theorem (e.g., Davenport [4, Ch. 5]; see also Uspensky and Heaslet [17, pp. 325–346]): to express a prime $p = 4k+1$ as $p = x^2 + y^2$ first express some multiple mp $(m < p)$ in that form, then reduce m, eventually to 1. The same proof suggests another deduction from (6). By careful choice of sign in (3), s and t in (8) are divisible by $M' := m_1 \cdots m_{I-1}$, and so for $U := s/M'$, $V := t/M'$ we have

$$U^2 + kV^2 = m_0 m_I. \tag{10}$$

We return to this later.

b) We can alternatively find m_0 as a prime of the form $m_0 = m + \nu n$ with $(-k/m_0) = 1$. Presumably such ν exists with $\nu = O(\log n)$ but we cannot prove this bound. This way to find m_0 seems to be more efficient in practice.

c) Instead of computing m_0, x_0 using a probabilistic square root algorithm, we can take $m_0 = 3 (\mathrm{mod}\, 4)$ and test $x_0 := (-k)^{(m_0+1)/4} (\mathrm{mod}\, m_0)$ for $x_0^2 = -k (\mathrm{mod}\, m_0)$. The latter equation is satisfied whenever m_0 is prime and $(-k/m_0) = 1$. This method fails if $k = j^2$ since $(-k/m_0) = -1$ for all primes $m_0 = 3 (\mathrm{mod}\, 4)$. So instead we take $m_0 = 5 (\mathrm{mod}\, 8)$ and test $x_0 := j \cdot 2^{(m_0-1)/4} (\mathrm{mod}\, m_0)$. This implies $x_0^2 = -k (\mathrm{mod}\, m_0)$ whenever m_0 is prime (see [9]).

IV. Occurrence of Noninvertible Elements

Some integers occurring in steps 2) and 4) of the algorithm must be relatively prime to n since their inverse $(\mathrm{mod}\, n)$ is used. These integers are $M = m_1 m_2 \cdots m_I$ in step 2) and y' in step 4) where we transform the solution x', y' of $x'^2 - m' y'^2 = -k (\mathrm{mod}\, n)$ into $y := 1/y'$, $x := x'/y' (\mathrm{mod}\, n)$. We discuss separately the cases $(M, n) \neq 1$ and $(y', n) \neq 1$. We assume that n is not a prime power since in this case we solve (1) by taking square roots in $\mathbb{Z}_n^*$, as is explained in the introduction.

Suppose $(M, n) \neq 1$. We cannot have $n | m_i$ since then $m_i = 0$ and $-k$ is a perfect square, $-k = j^2$, and thus the previous step 3) would stop with $m' = j^2$ (and initially $k > 0$). If $(m_i, n) \neq 1$, $n \nmid m_i$, we obtain a factorization of n into relatively prime factors $n_\nu, \nu = 1,2\cdots$. We continue to solve (1) separately for each modulus n_ν, and we combine the solutions by the Chinese remainder construction. We may have $n_\nu | m_i$ and thus $x_i^2 = -k (\mathrm{mod}\, n_\nu)$. In this case we solve $x^2 - y'^2 = m' (\mathrm{mod}\, n_\nu)$ by Lemma 1 below. This yields a solution $y = y'/x_i (\mathrm{mod}\, n_\nu)$ of $x^2 + ky^2 = m' (\mathrm{mod}\, n_\nu)$ which can be retraced to a solution of the original equation with modulus n_ν. Here we need $(k, n_\nu) = 1$ for the inversion of x_i, and $2 \nmid (m', n_\nu)$ for the application of Lemma 1.

Now suppose $(y', n) \neq 1$ in step 4) with $x'^2 - m' y'^2 = -k (\mathrm{mod}\, n)$. If $n \nmid y'$ we obtain a factorization of n into relatively prime factors $n_\nu, \nu = 1/2\cdots$. We continue to solve (1) separately for each modulus n_ν. If however $n | y'$ then $x'^2 = -k (\mathrm{mod}\, n)$. In this case we solve $x^2 - y''^2 = m' (\mathrm{mod}\, n)$ by Lemma 1 below. This yields a solution x, $y := y''/x' (\mathrm{mod}\, n)$ of $x^2 + ky^2 = m' (\mathrm{mod}\, n)$ that is needed in step 3). This step requires $(k, n) = 1$ in order to invert x', and $2 \nmid (m', n)$ for the application of Lemma 1.

We finally verify that after eliminating the case $(M, n) \neq 1$ in the described way, the current values for k and m remain relatively prime to n throughout the algorithm. The initial values k, m have this property. The only changes on k, m occur when k, m' are reduced to $-m', -k$ in step 4) and when, at the end of step 2), $m' = m_I$ is chosen for the new m. We have explained above that the algorithm continues with m' only if $(m', n) = 1$.

Lemma 1: If either n or m are odd the equation $x^2 - y^2 = m (\mathrm{mod}\, n)$ can be solved as $(r + 1/2)^2 - (r - 1/2)^2 = m (\mathrm{mod}\, n)$ with $r = m$, or $r = m + n$, whichever is odd.

Remark: The condition "n or m odd" cannot be removed. The equation $x^2 - y^2 = 2 (\mathrm{mod}\, 4)$ is unsolvable since x^2, y^2 are either 0 or $1 (\mathrm{mod}\, 4)$. It follows that $x^2 - y^2 = m (\mathrm{mod}\, 2^e)$ is unsolvable for $e \geq 2$ and $m = 2 (\mathrm{mod}\, 4)$; it can easily be solved in all other cases. It follows from the Chinese remainder theorem that $x^2 - y^2 = m (\mathrm{mod}\, n)$ is solvable iff either $4 \nmid m - 2$ or $4 \nmid n$.

V. Estimation of the Running Time

We first bound $E(n)$, the expected number of random pairs $u, v \in \mathbb{Z}_n$ that are tested in step 2) until $m_0 := m(u^2 + kv^2) (\mathrm{mod}\, n)$ is prime and $(-k/m_0) = 1$. For $m \in \mathbb{Z}_n^*$, $u^2 + kv^2 (\mathrm{mod}\, n)$ and m_0 are uniformly distributed over $\mathbb{Z}_n^*$. Therefore, $E(n) = O(n/\pi_{-k}(n))$ where $\pi_{-k}(n) = \#\{\text{primes } p \leq n \text{ with } (-k/p) = 1\}$. We know from the effective version of the Chebotarev density theorem (see Lagarias and Odlyzko [8, theorem 1]) that if the generalized Riemann hypothesis (GRH) holds for the zeta function of $Q(\sqrt{-k})$, then for all n,

$$\left| \pi_{-k}(n) - \frac{1}{2} Li(n) \right| < c\left(\sqrt{n} \log |kn|\right)$$

where c is an effectively computable constant, $Li(n) = \int_2^n dx/\log x$, and log is the natural logarithm.

If GRH holds then on the average there is at least one prime m_0 with $(-k/m_0) = 1$ for $O(\log n)$ random pairs

u, v. For such a prime m_0 the probabilistic square root algorithm finds $x_0 = \pm\sqrt{k} \pmod{m_0}$ with probability $\geq 1/2$ within $O(\log n)$ arithmetical operations over $\mathbb{Z}_{m_0}$. Thus the expected number of arithmetical steps for finding x_0, m_0 is at most $O(\log n)^2$. This dominates the $O(\log n)$ steps for the iteration (6) and for computing the inverse$(\bmod n)$. Each repetition of steps 2), 3), 4) of the algorithm halves the number of bits of $|k|$. Therefore steps 2), 3) 4) are repeated at most $O(|\log\log|k||)$ times. Thus the algorithm takes an expected number of $O((\log n)^2|\log\log|k||)$ arithmetical operations on $O(\log n)$-bit integers. If the algorithm splits the modulus n into relatively prime factors $n_\nu, \nu = 1, 2, \cdots$, we count a sequence of operations on $O(\log n_\nu)$-bit integers for $\nu = 1, 2, \cdots$ as one operation on an $O(\Sigma_\nu \log n_\nu)$-bit integer.

Theorem 2: Suppose GRH holds. Then, upon input k, m and n with $(km, n) = 1$, the proposed probabilistic algorithm solves $x^2 + ky^2 = m \pmod n$ with an expected number of $O((\log n)^2|\log\log|k||)$ arithmetical operations on $O(\log n)$-bit numbers.

Remarks: a) The condition $k, m \in \mathbb{Z}_n^*$ is necessary since the algorithm does not solve the equations $x^2 = m \pmod n$, $x^2 + ky^2 = 0 \pmod n$, $x^2 - y^2 = 2 \pmod 4$. Solving the equation $x^2 = m \pmod n$ for arbitrary $m \in \mathbb{Z}_n^*$ is as hard as factoring n; the equation $x^2 - y^2 = 2 \pmod 4$ is unsolvable.

b) It can easily be seen that an arbitrary nonlinear quadratic equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \pmod n,$$

with $a, b, c, d, e, f \in \mathbb{Z}$, can be reduced in $O(1)$ arithmetical steps to either an equation of type (1) or to an equation that is linear in one variable—and thus can easily be solved, or to an equation of type $x^2 = k \pmod n$. Therefore the algorithm for solving (1) solves arbitrary nonlinear quadratic equations mod n in two variables provided that the equation is not equivalent to $x^2 = k \pmod n$ for some k.

VI. Connections with Lattice Basis Reduction

The iteration (6) of the main step can be done in a somewhat more direct way by reducing an appropriate lattice basis of dimension 2 by either the Gaussian or the Lovász reduction algorithm [10]. This has independently been observed by J. Shallit [16].

When given x_0, m_0, m_1 such that $x_0^2 + k = m_0 m_1$, we can alternatively find $m' = m_I$ by minimizing the binary quadratic form

$$f(v, w) = (x_0 v + w m_1)^2 + kv^2$$

over integers $(v, w) \in \mathbb{Z}^2 - (0, 0)$. We have $f(v, w) = 0 \pmod{m_1}$ for all v, w in $\mathbb{Z}$, and thus we take $m' := f(v, w)/m_1$. Minimizing f is equivalent to minimizing the form

$$u^2 + kv^2$$

over the lattice $\{(u, v) \in \mathbb{Z}^2 : x_0 v = u \pmod{m_1}\}$.

If $k > 0$, the minimum is given by a shortest nonzero vector (in Euclidean length) $(u, \sqrt{k}\, v)$ of the lattice

$$L = \{(u, \sqrt{k}\, v) | x_0 v = u \pmod{m_1}\}$$

with determinant $d(L) = \sqrt{k}\,|m_1/\gcd(x_0, m_1)|$. By a well-known result $u^2 + kv^2 \leq \sqrt{4/3k}\,|m_1|$. This gives a solution $u, v, m' \in \mathbb{Z}$ of the equation

$$u^2 + kv^2 = m_1 m', \qquad 0 < m' \leq \sqrt{\frac{4}{3}k}\,.$$

If $k < 0$, a shortest nonzero vector of the lattice

$$L = \{(u, \sqrt{|k|}\, v) | x_0 v = u \pmod{m_1}\}$$

satisfies $u^2 + |k|v^2 \leq \sqrt{4/3|k|}\,|m_1|$ and gives a solution of the equation

$$u^2 + kv^2 = m_1 m', \qquad |m'| \leq \sqrt{\frac{4}{3}|k|}\,.$$

From a reduced basis b_1, b_2 of the lattice L we even obtain integers u, v such that $|u^2 + kv^2| \leq |m_1|\sqrt{|k|}$, and thus we achieve the bound $|m'| \leq \sqrt{|k|}$. It is sufficient to try all vectors $u + \sqrt{|k|}\, v$ in $\{b_1, b_2, b_1 + b_2, b_1 - b_2\}$. To prove the claim we consider the lattice

$$\bar{L} = \{(u, v) : x_0 v = u \pmod{m_1}\}$$

with determinant $d(\bar{L}) = |m_1/\gcd(x_0, m_1)|$. By Minkowski's convex body theorem (e.g., Cassels [3, Ch. III, 2.2]) there is a nonzero lattice point in the rhombus

$$R: |u + \sqrt{|k|}\, v| + |u - \sqrt{|k|}\, v| \leq 2\left(|m_1|\sqrt{|k|}\right)^{\frac{1}{2}}$$

of volume $V(R) = 4m_1$. By the arithmetic-geometric mean inequality one gets $|u^2 + kv^2| \leq |m_1|\sqrt{|k|}$ which solves the equation

$$u^2 + kv^2 = m_1 m', \qquad |m'| \leq \sqrt{|k|}\,.$$

Now the claim holds since the vectors $\pm b_1, \pm b_2, \pm(b_1 + b_2), \pm(b_1 - b_2)$ exhaust all points of the lattice L in the rhombus R.

In any case, the equations

$$x_0^2 + k = m_1 m' \qquad u^2 + kv^2 = m_1 m'$$

serve the same purpose as all the equations in (6). We can find u, v, m' by reducing the basis

$$(x_0, \sqrt{|k|}), (m_1, 0)$$

of the lattice L. A reduced basis $B = \{b_1, b_2\}$ can be found by the Gaussian reduction algorithm within $O(\log n)$ arithmetical operations on $O(\log n)$-bit integers.

VII. Connections with Legendre's Equation

The following is given by Mordell [11, p. 164].

Theorem 3: If the congruence

$$ak^2 + b = 0 \pmod m$$

is solvable, integers x, y, not both zero, exist such that

$$ax^2 + by^2 = Mm$$

for some integer M with $M < 2\sqrt{ab}$ if $a > 0$, $b > 0$, and $|M| < \sqrt{|ab|}$ if $ab < 0$.

We can add "given b, m and k, we can find M, x and y in polynomial time." For $a = 1$ we have shown this in (10) above. For $a \neq 1$ the claim follows from the equation $(ak)^2 + ab = 0 (\mathrm{mod}\ am)$ by applying the case $a = 1$. Alternatively we can find M, x and y, following the method of Section VI, by minimizing the quadratic form $f(u, v) = a^2(uk + vm_1)^2 + abu^2$, where m_1 is defined by $ak^2 + b = mm_1$.

Another solution of (1) is possible from the theory, due to Legendre, of the equation

$$ax^2 + by^2 + cz^2 = 0$$

(see Mordell [11, Ch. 7]). In outline this is rather simple:

1) transform k and m into equivalent odd primes k' and m' with $(m'/k') = (-k'/m') = 1$;
2) solve in integers the equation $x^2 + k'y^2 = m'z^2$;
3) deduce the solution $x' = x/z$, $y' = y/z (\mathrm{mod}\ n)$ of (1).

For an efficient transformation from k, m to k', m' in step 1) we can use the methods of the previous algorithm but we cannot rigorously analyze this step. Then following Cassels [3, Ch. III, 7.4] we can solve the equation of step 2) in probabilistic polynomial time. We first find square roots

$$a = \sqrt{-k'}\ (\mathrm{mod}\ m') \qquad b = \sqrt{m'}\ (\mathrm{mod}\ k').$$

All points of the lattice

$$L = \left\{ (x, y, z) \in \mathbb{Z}^3 : \begin{matrix} x = ya (\mathrm{mod}\ m'),\ x = zb (\mathrm{mod}\ k') \\ x = y (\mathrm{mod}\ 2),\ z = 0 (\mathrm{mod}\ 2) \end{matrix} \right\}$$

satisfy $x^2 + k'y^2 - m'z^2 = 0 \bmod(4k'm')$. The lattice has determinant $d(L) = 4|k'm'|$. By Minkowski's convex body theorem (see, e.g., Cassels [3, Ch. III, 2.2]), there is a nonzero lattice point in the ellipsoid

$$E: x^2 + |k'|y^2 + |m'|z^2 < 4|k'm'|$$

of volume $V(E) = (\pi/3)2^5|k'm'| > 2^3 d(L)$. This lattice point must satisfy $x^2 + k'y^2 - m'z^2 = 0$. We can find this lattice point by reducing a basis of lattice L.

Comparing with the algorithm of Section II we see that the new algorithm requires a more subtle initial transformation of k, m; then the whole recursion of the previous algorithm simplifies to reducing an appropriate lattice basis of some lattice L with algebraic coefficients contained in $\mathbb{R}^3$.

VIII. Solution of $X^2 + KZ^2 = M (\mathrm{mod}\ n)$ for Quadratic Integers

It has been asked in Ong, Schnorr, and Shamir [13] whether (1) can be solved efficiently for quadratic integers since otherwise this yields a very efficient public signature scheme. We extend the previous algorithm to the generalized equation.

For integers d, n we consider the ring $\mathbb{Z}_n[\sqrt{d}] := \mathbb{Z}[\sqrt{d}]/n\mathbb{Z}[\sqrt{d}]$. An element of $a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is *invertible* modulo $n\mathbb{Z}[\sqrt{d}]$ iff $a^2 - db^2$, the *norm* of $a + b\sqrt{d}$, is relatively prime to n. Let $\mathbb{Z}_n[\sqrt{d}]^*$ be the subgroup of $\mathbb{Z}_n[\sqrt{d}]$ consisting of the invertible elements. We will abbreviate $\mathrm{mod}(n\mathbb{Z}[\sqrt{d}])$ as $\mathrm{mod}\ n$.

For given elements K, M in $\mathbb{Z}[\sqrt{d}]$ that are invertible $\mathrm{mod}\ n$, we wish to solve the equation

$$X^2 + KY^2 = M (\mathrm{mod}\ n) \tag{11}$$

with X, Y in $\mathbb{Z}[\sqrt{d}]$. Let $M = m_1 + m_2\sqrt{d}$ and $K = k_1 + k_2\sqrt{d}$.

Outline of the Algorithm

1) If $n = p^e$ is a prime power we solve (11) directly by taking square roots in $\mathbb{Z}_{p^e}[\sqrt{d}]^*$.
2) Either split n or reduce (11) to the case that $m_2 \in n\mathbb{Z}$, $m_1 \in \mathbb{Z}_n^*$.
3) Either split n or reduce (11) to the case that $k_2, m_2 \in n\mathbb{Z}$, $k_1, m_1 \in \mathbb{Z}_n^*$.
4) Solve $x^2 + k_1y^2 = m_1 (\mathrm{mod}\ n)$ with $x, y \in \mathbb{Z}$ by the algorithm of Section II.
5) Work back to a solution of the original equation.

We explain the steps in more detail.

Step 1: Pick a random Y in $\mathbb{Z}_{p^e}[\sqrt{d}]$. Then the element $M - KY^2 (\mathrm{mod}\ p^e)$ is, with probability at least $1/2$, a square. If so, we can find a square root in probabilistic polynomial time since we are given the order of the group $\mathbb{Z}_{p^e}[\sqrt{d}]^*$, which is $p^{2e} - 1$ in case $(d/p) = -1$ and $p^{2e} - p^e$ in case $(d/p) = 1$.

Step 2: Let $M^{-1} = \overline{m}_1 + \overline{m}_2\sqrt{d}\ (\mathrm{mod}\ n)$. We assume that the numbers $\overline{m}_2, \overline{m}_2k_1 + \overline{m}_1k_2$ are either in $n\mathbb{Z}$ or in $\mathbb{Z}_n^*$; otherwise we split n. In particular we can assume that $\overline{m}_2 \in \mathbb{Z}_n^*$. We find $X, Y \in \mathbb{Z}[\sqrt{d}]$ and an integer m that is not in $n\mathbb{Z}$ such that

$$X^2 + KY^2 = Mm (\mathrm{mod}\ n). \tag{12}$$

This either reduces (11) to the equation $X'^2 + KY'^2 = m (\mathrm{mod}\ n)$, or splits n in case $m \notin \mathbb{Z}_n^*$. Equation (12) can be written as a quadratic equation for the integer coordinates of $X = x_1 + \sqrt{d}\,x_2$, $Y = y_1 + \sqrt{d}\,y_2$:

$$\begin{aligned} f(y_1, y_2) &:= (\overline{m}_2k_1 + \overline{m}_1k_2)(y_1^2 + dy_2^2) \\ &\quad + 2y_1y_2(\overline{m}_1k_1 + d\overline{m}_2k_2) \\ &= \overline{m}_2(x_1 + \overline{m}_1/\overline{m}_2x_2)^2 \\ &\quad + \overline{m}_2(d - \overline{m}_1^2/\overline{m}_2)x_2^2 (\mathrm{mod}\ n). \end{aligned} \tag{13}$$

If $KM^{-1} (\mathrm{mod}\ n)$ is a rational integer we solve (12) with $X = 0$, $Y = M$. In all other cases we have $\overline{m}_2k_1 + \overline{m}_1k_2 \in \mathbb{Z}_n^*$, and thus we can choose y_1, y_2 such that $f(y_1, y_2) \in \mathbb{Z}_n^*$. Then if $d - \overline{m}_1^2/\overline{m}_2 \in \mathbb{Z}_n^*$, we can solve the remaining equation in x_1, x_2 by the algorithm of Section II. If $d = \overline{m}_1^2/\overline{m}_2 (\mathrm{mod}\ n)$ we solve (13) with $y_1 = y_2 = 0$ and $x_1 = -x_2\overline{m}_1/\overline{m}_2 (\mathrm{mod}\ n)$; we can choose x_2 such that $m' \notin n\mathbb{Z}$.

Step 3: Since the equation $X^2 + KY^2 = m \pmod n$ is equivalent to $(X/Y)^2 - mY^{-2} = -K \pmod n$ we apply step 2) to the latter equation.

Steps 4 and 5 are straightforward. If we split n we can split n into relatively prime factors n_ν, $\nu = 1, 2, \cdots$. In this case we solve (11) separately for each modulus n_ν, and we combine the solution by the Chinese remainder construction.

So far we have reduced (11) to (1), and thus we can enunciate the following theorem.

Theorem 4: Suppose that GRH holds. For K, M in $\mathbb{Z}[\sqrt{d}]$ with K, M invertible modulo $n\mathbb{Z}[\sqrt{d}]$, we can solve (11) probabilistically using an expected number of $O((\log n)^2 \log\log n)$ arithmetical operations on $O(\log n)$-bit integers.

IX. Solution of the Equation $x^3 + ky^3 + k^2z^3 - 3kxyz = m \pmod n$.

If the above equation was difficult to solve for given k, m and n it would give an efficient signature scheme. It has been observed by Ong, Schnorr, and Shamir that there is an easy solution of the equation when given integers u and w satisfying

$$u^3 = k \pmod n \qquad w^3 = 1 \pmod n$$
$$1 + w + w^2 = 0 \pmod n.$$

By the discrete Fourier transform

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} := \begin{bmatrix} w, & w^2, & 1 \\ w^2, & w, & 1 \\ 1, & 1, & 1 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} \tag{14}$$

we have

$$x_1x_2x_3 = \prod_{i=1}^{3} \left(\sum_{j=1}^{3} w^{ij} s_j \right) = \sum_{i=1}^{3} s_i^3 = 3s_1s_2s_3.$$

To solve the equation

$$g(k, x, y, z) := x^3 + ky^3 + k^2z^3 - 3kxyz = m \pmod n \tag{15}$$

we first find integers x_1, x_2, x_3 such that $x_1x_2x_3 = m \pmod n$. Then we invert the transformation (14)

$$\begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix} := \frac{1}{3} \begin{bmatrix} w^2, & w, & 1 \\ w, & w^2, & 1 \\ 1, & 1, & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \pmod n,$$

and put $(x, y, z) := (s_1, s_2u^{-1}, s_3u^{-2}) \pmod n$.

If (15) was difficult to solve without knowing u then we could use this equation for verifying a signature (x, y, z) for the message m. We could use the private key u for signature generation and the public key k for signature verification.

We show, however, that there is an easy solution for (15). The quadratic form $g(k, x, y, z)$ is the norm,

$$g(k, x, y, z) = N(x + \zeta uy + \zeta^2 u^2 z), \tag{16}$$

of the number $x + \zeta uy + \zeta^2 u^2 z$ in the cubic field $Q(\zeta)$ where $\zeta \in \mathbb{R}$ is a primitive cube root of unity. Therefore we can compose solutions x_i, y_i, z_i of $g(k, x_i, y_i, z_i) = m_i$ for $i = 1, 2$ to a solution x, y, z of $g(k, x, y, z) = m_1m_2$ by writing

$$\begin{aligned} x &= x_1x_2 + k(y_1z_2 + y_2z_1) \\ y &= x_1y_2 + x_2y_1 \\ z &= x_1z_2 + z_1x_2 + y_1y_2. \end{aligned} \tag{17}$$

These equations in (17) are equivalent to

$$x + \zeta uy + \zeta^2 u^2 z = (x_1 + \zeta uy_1 + \zeta^2 u^2 z_1)(x_2 + \zeta uy_2 + \zeta^2 u^2 z_2).$$

Note that we can also compose a solution of $g(k, x, y, z) = m_1/m_2 \pmod n$ provided that $(m_2, n) = 1$.

In order to solve (15) it is sufficient to find integers a, b, c, d that solve the equation

$$\frac{a^3 + kb^3}{c^3 + kd^3} = m \pmod n. \tag{18}$$

This gives a solution

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{c^3 + kd^3} \begin{bmatrix} ac^2 + kbd^2 \\ -a(ad - bc) \\ d(ad - bc) \end{bmatrix} \pmod n.$$

For these integers x, y, z one can easily verify the equation

$$\frac{a + ub\zeta}{c + ud\zeta} = x + u\zeta y + u^2\zeta^2 z.$$

Thus by (16) these integers solve (15).

Conversely, given integers x, y, z that solve (15) we can solve (18) with

$$c = -y, \qquad d = z, \qquad b = xy - y^2, \qquad a = kz^2 - xy.$$

By the above transformations we can also compose solutions of (18) with right-hand sides m_1 and m_2 to solutions with right-hand sides m_1m_2 and $m_1/m_2 \pmod n$.

In (18) we can replace the pair (k, m) by $(-m, -k)$ since (18) is equivalent to the equation

$$\frac{a^3 - mc^3}{b^3 - md^3} = -k \pmod n.$$

The same replacement is possible for (15).

Now we can outline a solution of (15) (or (18)) which is similar to the previous solution of (1).

1) If n is a pure prime power then solve the equation by computing cube roots modulo n.
2) Replace m by an equivalent m' such that $|m'| \le |k|/2$.
3) If either m' is a perfect cube or $m' = k$, solve the equation $g(k, x, y, z) = m' \pmod n$ with $z = 0$ and either $y = 0$ or $x = 0$.
4) Apply the algorithm recursively to solve $g(-m', x, y, z) = -k \pmod n$.
5) Work back to a solution of the original equation.

The main step, step 2), needs further explanation. We can first transform m into an equivalent prime m_0; e.g., we test for primality: either $m_0 = m + \nu n$ for small integers ν, or $m_0 = mt^3 \pmod n$ for random t in $\mathbb{Z}_n^*$. By computing a cube root of $k \pmod{m_0}$ we find integers x_0, y_0, m_0 such that

$$x_0^3 + ky_0^3 = m_0 m_1.$$

Next we generate integers x_i, y_i, m_{i+1} for $i = 1, \cdots, I-1$ such that

$$x_i^3 + ky_1^3 = m_i m_{i+1} \tag{19}$$

and $|m_I| \le |k|/2$. From these integers and from a solution x', y', z' of $g(k, x', y', z') = m_I \pmod n$ we can compose a solution x, y, z of $g(k, x, y, z) = m_0 \pmod n$.

When given x_{i-1}, y_{i-1}, m_i, we find m_{i+1} with $|m_{i+1}| \le (27/23)^{1/4}\sqrt{|km_i|}$ by minimizing in absolute value the binary cubic form

$$f(v, w) = (vw_{i-1} + wm_i)^3 + v^3 k \tag{20}$$

over the pairs of integers (v, w) in $\mathbb{Z}^2 - (0,0)$. We have $f(v, w) = 0 \pmod{m_i}$ for all integers v, w. Since the form f has negative discriminant $\Delta = -27k^2|m_i|^6$ one can reduce f by an algorithm that is similar to the reduction of positive definite forms, i.e. to lattice basis reduction (see Cassels [3, Ch. II, 5.1 and 5.4]). From the reduced form one obtains integers v, w such that

$$|f(v, w)| \le \left(\frac{|\Delta|}{23}\right)^{1/4} = \left(\frac{27}{23}\right)^{1/4} \sqrt{|k|}\,|m_i|^{1.5}$$

(see Cassels [3, Ch. II, 5.4, Theorem IX]). This yields

$$|m_{i+1}| \le |f(v, w)|/|m_i| \le \left(\frac{27}{23}\right)^{1/4} \sqrt{|k|\,|m_i|}\,.$$

By repeating this process $O(\log n)$ times we find integers x_{I-1}, y_{I-1}, m_I such that

$$x_{I-1}^3 + ky_{I-1}^3 = m_{I-1} m_I, \qquad \text{with } |m_I| \le \sqrt{\frac{27}{23}}\,|k|.$$

In order to obtain $|m_I| \le |k|/2$ we repeat the iteration (19) several times starting with randomized values $mt^3 \pmod n$ instead of m.

Time analysis: Steps 3) and 4) are passed at most $O(\log n)$ times during the recursion. The length I of the iteration (19) is at most $O(\log\log|k|)$. Suppose for simplicity that 3 does not divide $\varphi(n)$, the order of the group $\mathbb{Z}_n^*$. Then $t \to mt^3 \pmod n$ is a 1-1 transformation of $\mathbb{Z}_n^*$, and in step 2) we can transform m into an equivalent prime m_0 in random polynomial time by checking whether $m_0 = mt^3 \pmod n$ is prime for about $O(\log n)$ random values t in $\mathbb{Z}_n^*$. We cannot rigorously prove that a few randomized initial values for m will decrease the final value of $|m_I|$ at the end of step 2) by about a factor of 2 beyond the bound $\sqrt{27/23}\,|k|$.

Modulo this assumption, the algorithm, upon input k, m and n with $(km, n) = 1$, solves (15) with an expected number of $O((\log n)^2 \log\log|k|)$ arithmetical operations on $O(\log n)$-bit integers.

Remarks

a) Minimizing the cubic form (20) over integers v, w is equivalent to minimizing the form

$$u^3 + kv^3$$

over the lattice $\{(u, v) \in \mathbb{Z}^2 : x_{i-1}v = u \pmod{m_i}\}$. For this we reduce the basis $(x_{i-1}, |k|^{1/3}m_i), (m_i, 0)$ of the lattice

$$L = \{(u, |k|^{1/3}v) \mid x_{i-1}v = u \pmod{m_i}\}$$

with determinant $d(L) = |m_i||k|^{1/3}/\gcd(x_{i-1}, m_i)$. Every nonzero vector $u + |k|^{1/3}v$ of this lattice which is shortest in the norm $u^3 + |k|v^3$ satisfies $u^3 + |k|v^3 \le (4/\pi)|m_i|^{1.5}\sqrt{|k|}$, since the convex set

$$C: u^3 + |k|v^3 \le \frac{4}{\pi}|m_i|^{1.5}\sqrt{|k|}$$

has volume $V(C) > 4d(L)$. This yields u, v, m_{i+1} such that

$$u^3 + kv^3 = m_i m_{i+1}, \qquad |m_{i+1}| \le \frac{4}{\pi}\sqrt{|m_i k|}\,,$$

and we finally obtain $|m_I| \le (4/\pi)^2|k|$. The constant $4/\pi$ can be decreased to $(27/23)^{1/4}$ by trying several of the short vectors in L.

b) There is another way to decrease $m' = m_I$ beyond the bound $|m'| \le \sqrt{27/23}\,|k|$ in step 2). We solve in advance all equations

$$g(p_i, x, y, z) = p_j \pmod n \tag{21}$$

where the integers p_i, p_j are either -1 or a prime less than 50. If the integer $m' = m_I$, obtained in step 2), has a prime factor p less than 50, we can take m'/p for the new m' and we solve directly the equation

$$g(k, x, y, z) = p \pmod n. \tag{22}$$

We replace (k, p) by $(-p, -k)$ and, following step 2) of the algorithm, we reduce (22) to an equation

$$g(-p, x, y, z) = \bar{m} \pmod n$$

with $|\bar{m}| \le \sqrt{27/23}\,p < 51$. Since $\bar{m}$ completely factors over primes less than 50 we can solve (22) by composing solutions of (21).

To solve (21) we pick for each of the 16 primes $p = p_i$ and $p = -1$ integers x_j, y_j, z_j for $j = 1, \cdots, 16$ and we put $m_j := g(p, x_j, y_j, z_j) \pmod n$. Following step 2) of the algorithm we reduce this to an equation

$$g(p, x_j', y_j', z_j') = m_j' \pmod n \tag{23}$$

with $|m_j'| \le \sqrt{27/23}\,|p| < 51$. Since m_j factors completely over the primes less than 51 we have $m_j' = \prod_\nu p_\nu^{d_{\nu,j}}$ with $d_{\nu,j} \in \mathbb{Z}$ for $j = 1, \cdots, 16$. If the matrix $(d_{\nu,j} \pmod 2)_{\nu,j}$ has rank 16, we find integers $u_{j,\mu}$ such that

$$\Sigma_j d_{\nu,j} u_{j,\mu} = \delta_{\nu,\mu} \pmod 2, \qquad \text{for } 1 \le \nu, \mu \le 16.$$

This yields $p_\mu = \prod_j (m'_j)^{u_{j,\mu}+2r_{j,\mu}}$ for some integers $r_{j,\mu}$, and thus we can solve the equation $g(p, x, y, z) = p_\mu \pmod n$ by composing solutions x'_j, y'_j, z'_j of (23).

Acknowledgment

We wish to thank the unknown referees for their comments. Section VI exploits hints of the referees; also the reference of Cassels [3, Ch. III, 7.4] for solving Legendre's equation was given by the referee.

References

[1] L. M. Adleman, K. Manders, and G. L. Miller, "On taking roots in finite fields," in *Proc. 18th Symp. on Foundation of Computer Science*, 1977, pp. 175–178.

[2] L. M. Adleman, D. Estes, and K. S. McCurley, "Solving bivariate quadratic congruences in random polynomial time," *Mathematics of Computation*, vol. 48, 1987.

[3] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, 2nd Ed. New York: Springer-Verlag, 1971.

[4] H. Davenport, *The Higher Arithmetic*, 5th Ed. Cambridge: Cambridge Univ., 1982.

[5] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Infom. Theory*, vol. IT-22 (1976), pp. 644–654.

[6] D. Estes, L. M. Adleman, K. Kompella, K. S. McCurley and G. L. Miller, "Breaking the Ong–Schnorr–Shamir signature scheme for quadratic number fields," in *Proc. Advances in Cryptology — Crypto' 85* (H. C. Williams, Ed.), Lecture Notes in Computer Science 218. New York: Springer-Verlag, 1986, pp. 3–13.

[7] J. C. Lagarias, "Worst-case complexity bounds for algorithms in the theory of integral quadratic forms," *J. Algorithms*, vol. 1, pp. 142–186, 1980.

[8] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem," in *Algebraic Number Fields, L-Functions, and Galois Properties*, A. Fröhlich, Ed. New York: Academic, 1977, pp. 409–464.

[9] D. H. Lehmer, "Computer technology applied to theory of numbers," in *Studies in Number Theory*, W. LeVeque, Ed. Englewood Cliffs, NJ: Prentice-Hall, 1969, pp. 117–151.

[10] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients," *Math. Annalen* 261 (1982), pp. 515–534.

[11] L. J. Mordell, *Diophantine Equations*. New York: Academic, 1969.

[12] H. Ong, C. P. Schnorr, and A. Shamir, "An efficient signature scheme based on quadratic equations," in *Proc. 16th Symp. on the Theory of Computing*, Washington, 1984, pp. 208–216.

[13] ____, "Efficient signature schemes based on polynomial equations," in *Proc. Advances in Cryptology — Crypto' 84* (G. R. Blakley and D. Chaum, Eds.), Lecture Notes in Computer Science 196. New York: Springer-Verlag, 1985, pp. 37–46.

[14] M. O. Rabin, "Probabilistic algorithms in finite fields," *SIAM J. Comp.* 9, 2 (1980), pp. 273–280.

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Comm. ACM*, vol. 21, pp. 120–126, 1978.

[16] J. Shallit, "An exposition of Pollard's algorithm for quadratic congruences," technical report, University of Chicago, 1984.

[17] J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*. New York: McGraw-Hill, 1939.