Attacks on the Birational Permutation Signature Schemes

Don Coppersmith
IBM Research
T. J. Watson Research Center
Yorktown Heights, NY 10598

Jacques Stern, Serge Vaudenay
Laboratoire d'Informatique
Ecole Normale Supérieure
75230 Paris, France

Abstract. Shamir presents in [3] a family of cryptographic signature schemes based on birational permutations of the integers modulo a large integer N of unknown factorization. These schemes are attractive because of the low computational requirements, both for signature generation and signature verification. However, the two schemes presented in Shamir's paper are weak. We show here how to break the first scheme, by first reducing it algebraically to the earlier Ong-Schnorr-Shamir signature scheme, and then applying the Pollard solution to that scheme. We then show some attacks on the second scheme. These attacks give ideas which can be applied to schemes in this general family.

1 The first scheme

The public information in Shamir's first scheme consists of a large integer N of unknown factorization (even the legitimate users need not know its factorization), and the coefficients of $k-1$ quadratic forms $f_2, \cdots, f_k$ in k variables $x_1, \cdots, x_k$ each. Each of these quadratic forms can be written as

$$f_i = \sum_{j,\ell} \alpha_{ij\ell} x_j x_\ell \tag{1}$$

where i ranges from 2 to k and the matrix $\alpha_{ij\ell}$ is symmetric i.e. $\alpha_{ij\ell} = \alpha_{i\ell j}$.

The secret information is a pair of linear transformations. One linear transformation B relates the quadratic forms $f_2, \cdots, f_k$ to another sequence of quadratic forms $g_2, \cdots, g_k$. The second linear transformation A is a change of coordinates that relates the variables $(x_1, \cdots, x_k)$ to a set of "original" variables $(y_1, \cdots, y_k)$. Denoting by Y the column vector of the original variables and by X the column vector of the new variables, we can simply write $Y = AX$.

Of course, the coefficients of A and B are known only to the legitimate user. The trap-door requirements are twofold: when expressed in terms of the original variables $y_1, \cdots, y_k$, the quadratic form g_2 is computed as:

$$g_2 = y_1 y_2 \tag{2}$$

and the subsequent g_i's, $3 \le i \le k$ are *sequentially linearized*, i.e. can be written

$$g_i(y_1, \cdots, y_k) = l_i(y_1, \cdots, y_{i-1}) \times y_i + q_i(y_1, \cdots, y_{i-1}) \tag{3}$$

D.R. Stinson (Ed.): Advances in Cryptology - CRYPTO '93, LNCS 773, pp. 435-443, 1994.

where l_i is a linear function of its inputs and q_i a quadratic form.

To sign a message M, one hashes M to a $k-1$-tuple $(f_2, \cdots, f_k)$ of integers modulo N, then finds a sequence $(x_1, \cdots, x_k)$ of integers modulo N satisfying (1). This is easy from the trap-door.

We let A_i, $2 \leq i \leq k$ denote the $k \times k$ symmetric matrix of the quadratic form f_i, namely:

$$A_i = (\alpha_{ij\ell})_{1 \leq j \leq k, 1 \leq \ell \leq k} \tag{4}$$

The kernel K_i of g_i is the kernel of the linear mapping whose matrix is A_i. It consists of vectors which are orthogonal to all vectors with respect to g_i. The rank of the quadratic form g_i is the rank of A_i. It is the dimension of K_i as well as the unique integer r such that g_i can be written as a sum of squares of r independent linear functionals. Actually, all this is not completely accurate as N is not a prime number and therefore $\mathbf{Z}/N$ is not a field. This question is addressed at the end the paper and, meanwhile, we ignore the problem.

An easy computation shows that K_i is the subspace defined in terms of the original variables by the equations

$$y_1 = \cdots = y_i = 0 \tag{5}$$

It follows from this that

i) K_i is decreasing

ii) the dimension of K_i is $k - i$

iii) any element of K_{i-1} not in K_i is an isotropic element wrt g_i, which means that the value of g_i is zero at this element.

We will construct a basis b_i of the k-dimensional space, such that $b_{i+1}, \cdots, b_k$ spans K_i for $i = 2, \cdots, k-1$. The main problem we face is the fact that the g_i's and therefore the K_i's are unknown. In place, we know the f_i's. We concentrate on the (unknown) coefficient δ_i of g_k in the expression of f_i, i.e. we write

$$f_i = \delta_i g_k + \sum_{j=2}^{k-1} \beta_{ij} g_j \tag{6}$$

As coefficients have been chosen randomly, we may assume that δ_k is not zero. Let $i < k$. Consider the quadratic form $Q_i(\lambda) = f_i - \lambda f_k$. When $\lambda = \delta_i/\delta_k$, this form has a non-trivial kernel and therefore δ_i/δ_k is a root of the polynomial $P_i(\lambda) = det(Q_i(\lambda))$. This is not enough to recover the correct value of λ. Computing the matrix of $Q_i(\lambda)$ for $\lambda_i = \delta_i/\delta_k$ in the basis corresponding to the original coordinates $y_1, \cdots, y_k$ yields the following

$$\begin{pmatrix} \boxed{\quad C \quad} & \boxed{0} \\ \boxed{\quad 0 \quad} & 0 \end{pmatrix}$$

In the same basis, the matrix of $Q_i(\lambda)$ for any λ, can be written as

$$\begin{pmatrix} \boxed{\quad C \quad} & \boxed{U_\lambda} \\ \boxed{(U_\lambda)^t} & 0 \end{pmatrix}$$

We observe that U_λ is linear in λ and vanishes at λ_i. Since determinants can be computed up to a multiplicative constant in any basis, it follows that $(\lambda-\lambda_i)^2$ factors out in $P_i(\lambda)$. Thus the correct value of λ_i can be found by observing that it is a double root of the polynomial equation $P_i(\lambda) = 0$. This double root is disclosed by taking the g.c.d. $\pmod N$ of P_i and P_i' with respect to λ. We find a linear equation in λ, from which we easily compute λ_i.

Once all coefficients λ_i have been recovered, we set for $i = 2, \cdots, k-1$

$$\tilde{f}_i = f_i - \lambda_i f_k \qquad i < k \tag{7}$$

and $\tilde{f}_k = f_k$. We note that all quadratic forms $\tilde{f}_i$ have kernel K_{k-1}. This allows to pick a non-zero vector b_k in K_{k-1}. The construction can then go on inductively in the quotient space of the k-dimensional space by the vector spanned by $\{b_k\}$ with $\tilde{f}_2, \cdots, \tilde{f}_{k-1}$ in place of $f_2, \cdots, f_k$.

At the end of the recursive construction, we obtain a sequence b_i, $3 \leq i \leq k$ such that $b_{i+1}, \cdots, b_k$ spans K_i for $i = 2, \cdots, k-1$ and a sequence of quadratic forms $\tilde{f}_2, \cdots, \tilde{f}_k$ such that

i) $\tilde{f}_i$ has kernel K_i

ii) b_i is an isotropic element wrt $\tilde{f}_i$

Choosing b_1, b_2 at random, we get another set of coordinates $z_1, \cdots, z_k$ such that

i) $\tilde{f}_2$ is a quadratic form in the coordinates z_1, z_2

ii) $\tilde{f}_3, \cdots, \tilde{f}_k$ is sequentially linearized

The rest is easy. From a sequence of prescribed values for $f_2, \cdots, f_k$, we can compute the corresponding values of $\tilde{f}_2, \cdots, \tilde{f}_k$. Next, we can find values of $\{z_1, z_2\}$ achieving a given value of $\tilde{f}_2 \pmod N$ in exactly the same way as the Pollard solution of the Ong-Schnorr-Shamir scheme [2]. Then, values for $z_3, \cdots, z_k$ achieving given values of $\tilde{f}_3, \cdots, \tilde{f}_k$ are found by successively solving $k-2$ linear equations. Finally, the values of $z_1, \cdots, z_k$ can be translated into values of $x_1, \cdots, x_k$.

Example. In Shamir's paper [3], an example is given with $N = 101$. (We use 101 to maintain consistency with Shamir's paper, even though 101 is prime, while N should be composite. We treat 101 as a number of unknown factorization; in particular we never solve nonlinear equations mod 101.)

$$v_2 = 78x_1^2 + 37x_2^2 + 6x_3^2 + 54x_1x_2 + 19x_1x_3 + 11x_2x_3 \pmod{101}$$

$$v_3 = 84x_1^2 + 71x_2^2 + 48x_3^2 + 44x_1x_2 + 33x_1x_3 + 83x_2x_3 \pmod{101}$$

Matrices of f_2, f_3 are as follows

$$\begin{pmatrix} 78 & 27 & 60 \\ 27 & 37 & 56 \\ 60 & 56 & 6 \end{pmatrix} \qquad \begin{pmatrix} 84 & 22 & 67 \\ 22 & 71 & 92 \\ 67 & 92 & 48 \end{pmatrix}$$

We get:

$$P(\lambda) = det(f_2 - \lambda f_3) = 34(\lambda^3 + 75\lambda^2 + 55\lambda + 71) \tag{8}$$

$$P'(\lambda) = \lambda^2 + 50\lambda + 52 \tag{9}$$

$$\gcd(P, P') = \lambda - 63 \tag{10}$$

We let

$$\tilde{f}_2 = f_2 - 63f_3 \quad ; \quad \tilde{f}_3 = f_3 \tag{11}$$

The kernel of $\tilde{f}_2$ is spanned by vector $b_3 = (31, 12, 1)^t$. We pick $b_2 = (0, 1, 0)^t$ and $b_1 = (1, 31, 0)^t$. We get, in the corresponding coordinates z_1, z_2, z_3:

$$\tilde{f}_2 = 26z_1^2 + 8z_2^2 \quad ; \quad \tilde{f}_3 = z_3(26z_1 + 20z_2) + 90z_1^2 + 2z_1z_2 + 71z_2^2 \tag{12}$$

2 The second scheme

We now treat Shamir's [3] second scheme. The ideas developed in this section will have general applicability.

Throughout, we will pretend we are working in $\mathbf{Z}/p$ rather than $\mathbf{Z}/N$.

We treat first the case $s = 1$. We begin with k variables $y_1, y_2, \ldots, y_k$, with k odd. These are subjected to a secret linear change of variables which gives $u_i = \sum_j a_{ij}y_j, i = 1, 2, \ldots, k$, with the matrix $A = (a_{ij})$ secret. The products u_iu_{i+1}, including u_ku_1, are subjected to a second secret linear transformation $B = (b_{ij})$, so that $v_i = \sum_j b_{ij}u_ju_{j+1}, i = 1, 2, \ldots, k-1$. The public key is the set of coefficients $(c_{ij\ell})$ expressing v_i in terms of pairwise products y_jy_ℓ, for $1 \le i \le k-1$,

$$v_i = \sum_{j,\ell} c_{ij\ell}y_jy_\ell, 1 \le i \le k-1, c_{ij\ell} = c_{i\ell j} \tag{13}$$

(Here i is ranging to $k-1$, so we have discarded $s = 1$ of the v_i.)

The first step in our solution: linear combinations of the v_i are linear combinations of the u_iu_{i+1}, but they form only a subspace of dimension $k-1$. Some linear combinations of the v_i,

$$v_1 + \delta v_2 + \sum_{3 \le j \le k-1} \epsilon_j v_j \tag{14}$$

will be quadratic forms in the y_i of rank 2. A computation shows that the only linear combinations of the products $u_i u_{i+1}$ of rank 2 are of the form

$$\alpha_i u_{i-1} u_i + \beta_i u_i u_{i+1} = u_i(\alpha_i u_{i-1} + \beta_i u_{i+1}), \tag{15}$$

for any values of α_i, β_i, i. Because the v_j span a subspace of codimension 1, and because we are further restricting to one lower dimension by the choice of the multiplier 1 for v_1 in the linear combination, we find that for each i there will be one pair (α_i, β_i) and one set of coefficients (δ, ϵ_j) such that

$$\alpha_i u_{i-1} u_i + \beta_i u_i u_{i+1} = u_i(\alpha_i u_{i-1} + \beta_i u_{i+1}) = v_1 + \delta v_2 + \sum_{3 \le j \le k-1} \epsilon_j v_j. \tag{16}$$

The condition of being rank 2 is an algebraic condition: setting

$$v_1 + \delta v_2 + \sum_{3 \le j \le k-1} \epsilon_j v_j = \sum_{ij} \tau_{ij} y_i y_j, \tag{17}$$

with $\tau_{ij} = \tau_{ji}$, we find that each 3×3 submatrix of the (τ_{ij}) has vanishing determinant. Each of these determinants is a polynomial equation in δ, ϵ_j. Use resultants to eliminate ϵ_j from this family of polynomial equations (in the ring $\mathbf{Z}/N$) and find a single polynomial F of degree k satisfied by δ. We also find ϵ_j as polynomials in δ, by returning to the original equations and eliminating the variables $\epsilon_i, i \neq j$.

Thus each solution δ to $F(\delta) = 0$ gives rise to a linear combination of v_j which is of rank 2. The root δ corresponds to that index i for which

$$v_1 + \delta v_2 + \sum_{3 \le j \le k-1} \epsilon_j v_j = u_i(\alpha_i u_{i-1} + \beta_i u_{i+1}). \tag{18}$$

We will indicate this correspondence by writing $\delta = \delta_i$.

For each solution $\delta = \delta_i$, the rows of the resulting matrix (τ_{ij}) span a subspace $Y(\delta_i) = Y_i$ of $\mathbf{Z}_p^k$ of rank 2; namely, Y_i is spanned by u_i and $\alpha_i u_{i-1} + \beta_i u_{i+1}$.

Observe that u_i, u_{i+2}, and $(\alpha_{i+1} u_i + \beta_{i+1} u_{i+2})$ are linearly related, as are u_i, u_{i-2}, and $(\alpha_{i-1} u_{i-2} + \beta_{i-1} u_i)$. So

$$u_i \in Y_i \cap (Y_{i+1} + Y_{i+2}) \cap (Y_{i-1} + Y_{i-2}) \tag{19}$$

This is an algebraic relation among δ_{i-2}, δ_{i-1}, δ_i, δ_{i+1}, and δ_{i+2}.

We formulate the relation as the vanishing of several determinants, and reduce the resulting ideal by factoring out any occurrences of $(\delta_i - \delta_j), i \neq j$ to assure that δ_i, δ_j are really two different solutions. That is, we consider the ideal formed by $F(\delta_i)$, $(F(\delta_i) - F(\delta_j))/(\delta_i - \delta_j)$, etc., and the various determinants. We apply the Groebner basis and the Euclidean algorithm to this ideal to find a basis.

Only multiples of some u_i satisfy such a relation (19) over $\mathbf{Z}/p$, namely, two different linear relations. We fix a multiple of each u_i by normalizing u_i to have first coordinate 1. The linear relations serve to define u_i in terms of δ_i.

By similar argument, there is a quadratic equation expressing δ_{i+1} in terms of δ_i, whose two solutions are δ_{i+1} and δ_{i-1}. The algebraic condition is that the corresponding spaces Y_i, Y_{i+1} are in two different triples of subspaces enjoying linear relations:

$$rank(Y_i + Y_{i+1} + Y_{i+2}) = rank(Y_i + Y_{i+1} + Y_{i-1}) = 5 \tag{20}$$

We represent the solution of the quadratic equation by τ, and say that (δ, τ) generates a pair of 'adjacent' elements (u_i, u_{i+1}) (elements which are multiplied together in the original signature). We think of δ as generating an extension of degree k over $\mathbf{Z}/N$, and τ as generating an extension of degree 2 over $\mathbf{Z}/N[\delta]/F(\delta)$. The ability to distinguish the unordered pairs of 'adjacent' roots $\{\delta_i, \delta_{i+1}\}$ makes the system similar, in spirit, to a Galois extension of $\mathbf{Q}$ whose Galois group is the dihedral group on k elements. We will call on this analogy later. (Remark: it is only an analogy, because δ and τ really are elements of the ground fields.)

We can get the missing kth equation

$$v'_k = \sum_i u_i u_{i+1}. \tag{21}$$

The coefficients of v'_k in terms of $y_j y_\ell$ ostensibly depend on δ_i and on the pairings (δ_i, δ_{i+1}), or equivalently on (δ, τ). But the coefficients would come out the same no matter which solution (δ, τ) were chosen, that is, no matter whether we assigned the ordering $(1, 2, 3, \ldots, k)$ or $(3, 2, 1, k, k-1, \ldots, 4)$ to the solutions u_i. This means that the coefficients will be in fact independent of (δ, τ). They will be expressible in terms of only the coefficients of the original $v_i, 1 \le i \le k$. This is because they are symmetric (up to dihedral symmetry) in the solutions δ_i.

The arguments here are analogous to those of Galois theory. Each coefficient c of v'_k is expressed as

$$c = \sum_{0 \le i < k, 0 \le j \le 1} w_{ij} \delta^i \tau^j \tag{22}$$

For each of $2k$ different choices of (δ, τ) the value of c comes out the same. Treating (22) as $2k$ linear equations in the $2k$ unknowns w_{ij}, with coefficients given by $\delta^i \tau^j$ for various choices of (δ, τ), we must find (if the matrix has full rank) that $w_{00} = c$, and $w_{ij} = 0$ for $(i, j) \ne (0, 0)$.

Now we wish to solve a particular signature. We are given the values $v_1, \ldots, v_{k-1}$, and we assign an arbitrary value to v'_k. We have the equations relating v_i to $u_j u_{j+1}$:

$$v_i = \sum_j b'_{ij} u_j u_{j+1}, \tag{23}$$

where b'_{ij} depends on δ_j. Select (symbolically) one pair (δ, τ) to fix the first two solutions (u_1, u_2), and compute the others in terms of (δ, τ). Then we have $b'_{ij} u_j u_{j+1}$ depending only on (δ, τ).

Invert this matrix b' to solve for $u_j u_{j+1}$ in terms of the given v_i and (δ, τ).

Now assign

$$u_1 = \xi, \tag{24}$$

where ξ is an unknown. Compute

$$u_2 = \frac{(u_1u_2)}{\xi}, u_3 = \frac{\xi(u_2u_3)}{(u_1u_2)}, u_4 = \frac{(u_1u_2)(u_3u_4)}{\xi(u_2u_3)}, \dots, u_1 = \frac{(u_1u_2)(u_3u_4)\dots(u_ku_1)}{\xi(u_2u_3)\dots(u_{k-1}u_k)} \tag{25}$$

The last equation gives a quadratic equation which ξ must satisfy:

$$(u_1u_2)(u_3u_4)\dots(u_ku_1) = \xi^2(u_2u_3)\dots(u_{k-1}u_k) \tag{26}$$

We do not solve for ξ (we cannot). So now we have three algebraic unknowns: δ, τ, ξ, of successive degrees $k, 2, 2$.

These equations give u_i in terms of δ, τ, ξ. Notice that each u_i is an odd function of ξ: either ξ times a function of (δ, τ) or ξ^{-1} times a function of (δ, τ). We also have u_i as linear combinations of y_j with coefficients depending on (δ, τ). Solve for y_j in terms of (δ, τ, ξ), and note that y_j is again an odd function of ξ.

Now each product y_jy_ℓ will be a function only on (δ, τ), since it will be an even function of ξ, and we know ξ^2 in terms of (δ, τ). But again the value y_jy_ℓ will be independent of the dihedral ordering $(1, 2, 3, \dots, k)$ versus $(3, 2, 1, k, k-1, \dots, 4)$, and thus independent of the choice of solutions (δ, τ). That means, by standard Galois theory arguments, that (δ, τ) will not appear in the expressions of y_jy_ℓ.

So we have found the products y_jy_ℓ in terms of the given coefficients, the given values $v_1, v_2, \dots, v_{k-1}$, and the assumed value v'_k. We have given a valid signature.

3 Comments and extensions

3.1 Working mod N versus working mod p

Some justification is needed to go from calculations mod$p$ to calculations mod N. In section 1, we basically use tools from linear algebra such as Gaussian elimination or determinants. Thus all computations go through regardless the fact that N is composite. The situation is a bit more subtle in section 2. For instance, F has k solutions mod$p$ but k^2 solutions mod$N$, each obtained by mixing some solution mod$p$ with some solution mod$q$. But if we consider only the image, $\bmod p$, of our calculations $\bmod N$, things are all right: the symmetric functions of the k roots of a polynomial are expressible in terms of the coefficients of the polynomial, and the expressions of the products y_jy_ℓ in terms of the coefficients of the public key are valid $\bmod p$. They are also valid $\bmod q$, and the Chinese remainder theorem suffices to make them valid mod$N$. This in spite of the fact that a solution δ of $F \bmod N$ might well mix different solutions $\delta_i \bmod p$ and $\delta_j \bmod q$. Since we never explicitly solve for δ, but only work with it symbolically and use the fact that $F(\delta) = 0 \bmod N$, we never are in danger of factoring N.

3.2 Extension to the case $s > 1$ (Sketch)

The case $s > 1$ is more complicated. Suppose again that we have k variables $y_1, y_2, \ldots, y_k$, with k odd, whose pairwise products constitute the signature, and that the hashed message has $k - s$ quantities $v_1, v_2, \ldots, v_{k-s}$, together with coefficients $c_{ij\ell}$ expressing v_i in terms of $y_j y_\ell$. Suppose for simplicity that $s > 1$ is odd, so that $k - s$ is even.

Some linear combinations of the $k - s$ quadratic forms v_i will have rank $s+1$. Namely, for each index set $I \subseteq \{1, 2, \ldots, k\}$ of size $(s+1)/2$ such that $\forall i, j \in I$: $|i - j| \geq 2$, there is such a linear combination of the form

$$\sum_{i \in I} u_i(\alpha_{iI} u_{i-1} + \beta_{iI} u_{i+1}) \tag{27}$$

The number of such index sets I is

$$\frac{k}{\frac{s+1}{2}} \binom{k - \frac{s+3}{2}}{\frac{s-1}{2}} \tag{28}$$

There are more than k linear combinations, leading to increased complication. The space Y_I, spanned by rows of the corresponding quadratic form, contains u_i for each index $i \in I$. So each u_i is in the intersection of a large number of subspaces Y_I, and hopefully only multiples of u_i will be in such an intersection. This algebraic condition should distinguish the u_i, hopefully indexing them by the roots δ of some polynomial $F(\delta)$ of degree k. Pairs $\{u_i, u_{i+2}\}$ of solutions with index differing by 2 should be distinguished by appearing together in many different subspaces Y_I. Using this we would be able to distinguish pairs $\{u_i, u_{i+1}\}$. We would fabricate the missing equations: for $j = k - s + 1, \ldots, k$, let $u'_{i(j)}$ be a multiple of u_i, normalized to have a 1 in position j, and set $v'_j = \sum_i u'_{i(j)} u'_{i+1(j)}$.

3.3 The case k=3, s=1

In the special case $k = 3$, $s = 1$, where we must satisfy two quadratic equations in three variables, we can employ an *ad hoc* method, since the methods outlined above don't work. Take a linear transformation of the two quadratic equations so that the right-hand side of one equation vanishes; that is, if the given values are v_1 and v_2, take v_2 times the first equation minus v_1 times the second. This gives a homogeneous quadratic equation in three variables y_1, y_2, y_3:

$$\sum_{ij} c_{ij} y_i y_j = 0 \tag{29}$$

The second equation is inhomogeneous:

$$\sum_{ij} d_{ij} y_i y_j = d_0 \tag{30}$$

By setting $z_1 = y_1/y_3$, $z_2 = y_2/y_3$ in (29), we obtain an inhomogeneous quadratic equation in two variables z_1, z_2. We can easily find an affine change of basis from z_1, z_2 to z_1', z_2' which transforms the equation to the form

$$c_{11}' {z_1'}^2 + c_{12}' z_1' z_2' + c_{22}' {z_2'}^2 = c_0' \bmod N \tag{31}$$

and a further linear change of variables to z_1'', z_2'' yielding

$$c_{11}'' {z_1''}^2 + c_{22}'' {z_2''}^2 = c_0'' \bmod N \tag{32}$$

which can be solved by the Pollard [2] attack on the Ong-Schnorr-Shamir [1] scheme. We find from this a set of ratios y_j/y_3, and, by extension, a set of ratios $y_i y_j / y_3^2$, satisfying (29). Setting $y_3^2 = \lambda$, the second equation (30) becomes a linear equation in λ. Thus we find a consistent set of pairwise products $y_i y_j$ satisfying the desired equations (29), (30).

3.4 Open questions

The birational permutation signature scheme has many instances, of which we have attacked only the first few examples. For a more complex instance of the scheme, the ideas of the present paper will still apply: the trap door conditions lead to algebraic equations on the coefficients of the transformations, and we hope to gather enough such equations to make it possible to solve them by g.c.d. or Groebner basis methods. But, for any specific instance, it remains to see whether the ideas of the present paper would be sufficient to mount an attack.

One general theme is that when solutions of the algebraic equations enjoy a symmetry, it makes the equations harder to solve, but we don't need to solve them, since the final solution will enjoy the same symmetry, and quantities symmetric in the roots of the equation can be expressed in terms of the coefficients of the equation alone, not in terms of the roots. When the roots fail to enjoy a symmetry, they can be distinguished by algebraic conditions, which yield further algebraic equations, and the Groebner basis methods have more to work with. This gives us hope that the methods outlined in this paper will apply with some generality to many instances of the birational permutation signature scheme.

References

1. H. Ong, C. P. Schnorr, and A. Shamir: A fast signature scheme based on quadratic equations. Proc. 16th ACM Symp. Theory of Computing, pp.208-216; 1984.
2. J. M. Pollard and C. P. Schnorr: An efficient solution of the congruence $x^2 + ky^2 = m$ (mod n). IEEE Trans. Inform. Theory vol IT-33 no 5, pp.702-709; Sept., 1987.
3. A. Shamir: Efficient signature schemes based on birational permutations. Manuscript March 1993. To appear, *Crypto 93*.