How to Break Shamir's Asymmetric Basis

Thorsten Theobald*

Fachbereich IV - Informatik, Universität Trier
D-54286 Trier, Germany
theobald@ti.uni-trier.de

Abstract. At Crypto 93, Shamir proposed a family of signature schemes using algebraic bases. Coppersmith, Stern and Vaudenay presented an attack on one variant of the cryptosystem. Their attack does not recover the secret key. For one of the variants proposed by Shamir we show how to recover the secret key. Our attack is based on algebraic methods which are also applicable to many other instances of polynomial equations in the presence of some trapdoor condition.

1 Introduction

In 1984, Ong, Schnorr and Shamir [OSS84] proposed a very efficient signature protocol based on a quadratic equation in two variables modulo a number of unknown factorization. The scheme was broken by Pollard [PS87], who developed an efficient algorithm to solve these congruences. His algorithm was a great breakthrough in determining the computational complexity of modular quadratic congruences.

Recently, there have been two attempts [Na93], [Sh93b] to repair the weaknesses of the OSS-protocol by inserting additional non-linear structures into the framework of polynomial equations. The low computational requirements of the resulting schemes were especially attractive for devices with restricted computational power. In order to demonstrate the strength of his scheme, Shamir [Sh93a] developed a formal theory concerning the difficulty of polynomial factorization modulo a composite number. From all the members of a very general family, Shamir recommended two variants of his signature scheme: a symmetric one and an asymmetric one.

The symmetric variant could be broken by Coppersmith, Stern and Vaudenay [CSV93]. They showed how to forge a signature, but the secret key is not revealed. However, the main starting point of their attack very strongly relies on the specific symmetry of the underlying algebraic basis[2]. It has been an open problem whether other members of the family are also vulnerable or not.

In this paper we present an attack on the asymmetric basis. Our results are quite unexpected. The asymmetric basis is not only weak in the sense that

* Supported by DFG-Graduiertenkolleg "Mathematische Optimierung". This work was done while the author was at the University of Frankfurt.

[2] An algebraic basis is a set of polynomials with some additional properties (see [Sh93b]).

D. Coppersmith (Ed.): Advances in Cryptology - CRYPTO '95, LNCS 963, pp. 136-147, 1995.

signatures can be forged. Moreover, it is even possible to recover the secret key within a very short time.

Our attack is based on a detailed analysis of the asymmetric basis polynomials. This characterization makes it possible to apply some ideas of [CSV93] even in the absence of symmetry: Algebraic conditions are transformed into polynomial equations. We then present a method that makes it even possible to solve the specific polynomial equations explicitly. From the solutions of the equations it is only a small step to recover the secret key.

Our attack does not only completely break Shamir's signature scheme. The presented methods also form general guidelines to attack polynomial equations in the presence of some trapdoor information. The connection of our methods with the above mentioned attacks on previous signature schemes provides powerful cryptanalytic tools. We hope that applications of these tools lead to further developments in the area of polynomial equations and in cryptographic research.

2 The signature scheme using algebraic bases

Let $k \geq 3$ and n be the product of two large secret primes p and q. All computations will be done in $\mathbb{Z}_n$, the ring of numbers modulo n. The set of polynomials $\{u_1^2, u_1u_2, u_2u_3, \ldots, u_{k-1}u_k\}$ is called the *asymmetric basis* ([Sh93b]).

Two secret invertible matrices $A, B \in \mathbb{Z}_n^{k,k}$ are used to mix up the polynomials. The matrix A transforms the original variables $u_1, \ldots, u_k$ into new variables $y_1, \ldots, y_k$:

$$u_i = \sum_{j=1}^{k} a_{ij} y_j, \quad 1 \leq i \leq k. \tag{1}$$

The matrix B defines k quadratic forms $v_1(u_1, \ldots, u_k), \ldots, v_k(u_1, \ldots, u_k)$ which are linear combinations of the basis elements:

$$v_i(u_1, \ldots, u_k) := b_{i1}u_1^2 + \sum_{j=2}^{k} b_{ij} u_{j-1}u_j, \quad 1 \leq i \leq k. \tag{2}$$

Applying the variable transformation (1) to the polynomials of (2) yields k homogenous quadratic forms $v_i'(y_1, \ldots, y_k)$, $1 \leq i \leq k$. The public key consists of the quadratic forms $v_i'(y_1, \ldots, y_k)$, $1 \leq i \leq k-1$. $v_k'(y_1, \ldots, y_k)$ is not published in order to prevent unique signatures.

A message m is represented by $k-1$ hash values $h_1(m), \ldots, h_{k-1}(m)$. Due to the basis property, each assignment of values (from $\mathbb{Z}_n$) to the basis elements y_1^2, $y_1y_2, \ldots, y_{k-1}y_k$ implies unique assignments to all homogeneous polynomials of degree 2 in $y_1, \ldots, y_k$. Such an assignment to $y_1^2, y_1y_2, \ldots, y_{k-1}y_k$ forms a valid signature for m if

$$v_i'(y_1, \ldots, y_k) = h_i(m), \quad 1 \leq i \leq k-1.$$

For a shorter notation, we write v_i instead of $v_i(u_1, \ldots, u_k)$ and v_i' instead of $v_i'(y_1, \ldots, y_k)$.

3 The attack

We address the algebraic problem of finding matrices $A', B' \in \mathbb{Z}_n^{k,k}$, which produce a given public key. The description of the attack refers to a prime modulus. We will justify at the end, why the methods also work in case of a composite modulus.

Throughout the attack, we will not consider degenerated cases which appear with probability of order $O(2^{-l(n)})$, where $l(n)$ is the bitlength of the modulus.

To make the signature scheme vulnerable by algebraic methods, the following definitions are helpful (see e.g. [Ja74]). With every homogeneous quadratic form $q(x_1, \ldots, x_k) \in \mathbb{Z}_n[x_1, \ldots, x_k]$, we associate a $k \times k$-matrix Q (Q is called the *matrix of q*):

$$Q_{j,l} := \begin{cases} \text{coefficient of } x_j x_l \text{ in } q, & j = l \\ \frac{1}{2} \cdot \text{coefficient of } x_j x_l \text{ in } q, & j \neq l \end{cases}.$$

Q is a symmetric matrix which satisfies

$$q(x_1, \ldots, x_k) = (x_1, \ldots, x_k)\, Q\, (x_1, \ldots, x_k)^T.$$

The *rank* of a homogeneous quadratic form is defined as the rank of the associated matrix. It can easily be checked that the rank of a quadratic form is invariant with respect to invertible linear variable transformations. For a matrix Q, the determinant of a $j \times j$-submatrix is called a *minor of order j*. The *row domain* of a matrix is the vector space spanned by the row vectors of the matrix.

3.1 Exploiting the trapdoor

A matrix, that is associated to a linear combination of the basis elements, has only very few nonzero entries. This fact will turn out to be the main weakness of the scheme. A precise classification of the linear combinations with low rank is given in the following lemma. The classification can be exploited in order to establish conditions about the rank of quadratic forms. A rigorous proof for lemma 1 can be found in the appendix.

Lemma 1. *Let $k \geq 4$. A linear combination of the basis elements u_1^2, $u_1 u_2$, ..., $u_{k-1} u_k$ is a quadratic form of rank not greater than 2 if and only if it is of the form*

$$\begin{aligned} & \alpha_1 u_1 u_2 + \beta_1 u_2 u_3 && \textit{(type 1)}, \\ & \alpha_2 u_2 u_3 + \beta_2 u_3 u_4 && \textit{(type 2)}, \\ & \vdots && \\ & \alpha_{k-2} u_{k-2} u_{k-1} + \beta_{k-2} u_{k-1} u_k && \textit{(type } k-2\textit{)} \\ \textit{or} \quad & \alpha_{k-1} u_1^2 + \beta_{k-1} u_1 u_2 && \textit{(type } k-1\textit{)} \end{aligned} \tag{3}$$

with $\alpha_i, \beta_i \in \mathbb{Z}_n$, $1 \leq i \leq k-1$.

Linear combinations of the polynomials $v_1, \ldots, v_{k-1}$ are linear combinations of the basis elements $u_1^2, u_1u_2, \ldots, u_{k-1}u_k$. The characterization from lemma 1 can be used to fix $k-1$ important coefficient tuples in these linear combinations.

Lemma 2. *The following system of $k-1$ equations with unknowns α_i, β_i, δ_i, $\epsilon_{3,i}, \ldots, \epsilon_{k-1,i}$, $i \in \{1, \ldots, k-1\}$, has a unique solution:*

$$\alpha_1 u_1 u_2 + \beta_1 u_2 u_3 = v_1 + \delta_1 v_2 + \sum_{j=3}^{k-1} \epsilon_{j,1} v_j,$$

$$\vdots$$

$$\alpha_{k-1} u_1^2 + \beta_{k-1} u_1 u_2 = v_1 + \delta_{k-1} v_2 + \sum_{j=3}^{k-1} \epsilon_{j,k-1} v_j.$$

Proof. It is sufficient to show: For each $i \in \{1, \ldots, k-1\}$ there exists exactly one pair $(\alpha_i, \beta_i) \in \mathbb{Z}_n^2$ and exactly one $(k-2)$-tuple $(\delta, \epsilon_3, \ldots, \epsilon_{k-1}) \in \mathbb{Z}_n^{k-2}$, such that the quadratic form of type i from (3) is equal to $v_1 + \delta v_2 + \sum_{j=3}^{k-1} \epsilon_j v_j$.

Consider the linear space V of the linear combinations $a_1 u_1^2 + \sum_{j=2}^{k} a_j u_{j-1} u_j$ for arbitrary $a_j \in \mathbb{Z}_n$, $1 \leq j \leq k$. The vector space V is of dimension k. The linear combinations of type i for arbitrary $\alpha_i, \beta_i \in \mathbb{Z}_n$ form a two-dimensional subspace U_i of V.

The quadratic forms $v_1 + \delta v_2 + \sum_{j=3}^{k-1} \epsilon_j v_j$ with arbitrary coefficients $\delta, \epsilon_3, \ldots, \epsilon_{k-1} \in \mathbb{Z}_n$ form an affine subspace T of dimension not greater than $k-2$ of V. The quadratic forms $v_1, \ldots, v_{k-1}$ are linearly independent, because the matrix B from (2) is invertible. Therefore $\dim T = k-2$. In the non-degenerated case, $U_i \cap T$ is of dimension zero. □

Consider now the algebraic condition

$$v_1 + \delta v_2 + \sum_{j=3}^{k-1} \epsilon_j v_j \text{ has a rank not greater than 2.} \tag{4}$$

A matrix is of rank not greater than 2 if and only if all minors of order 3 vanish. If the quadratic forms $v_i = v_i(u_1, \ldots, u_k)$, $1 \leq i \leq k-1$, were known, then condition (4) could be expressed as the vanishing of several determinants with unknowns $\delta, \epsilon_3, \ldots, \epsilon_{k-1}$.

Of course, the polynomials $v_i = v_i(u_1, \ldots, u_k)$, $1 \leq i \leq k-1$, are not part of the public key. However, due to the invariance of the rank with respect to invertible linear variable transformations the condition (4) is equivalent to

$$v_1' + \delta v_2' + \sum_{j=3}^{k-1} \epsilon_j v_j' \text{ has a rank not greater than 2.} \tag{5}$$

Condition (5) can be transformed into a system of polynomial equations: For the matrix of the quadratic form in (5), each minor of order 3 vanishes. The minors

are polynomials in $\delta, \epsilon_3, \ldots, \epsilon_{k-1}$. It is possible to use algebraic standard techniques like resultants and the Gaussian elimination algorithm (see e.g. [Mi93]) in order to obtain
1. polynomial expressions for $\epsilon_3, \ldots, \epsilon_{k-1}$ in terms of δ.
2. a polynomial $P(\delta)$ of degree k with simple zeros $\delta_1, \ldots, \delta_{k-2}$ and a double zero δ_{k-1}, where $\delta_1, \ldots, \delta_{k-1}$ are defined as in lemma 2.
For further details of the technical elimination process, see [The95].

Remark. The essential reason why δ_{k-1} must be a double zero of the computed polynomial $P(\delta)$ is the following: In the matrix associated with the quadratic form of type $k-1$ from (3) each submatrix of order 3 consists of at least one row and one column in which only zeros appear. Therefore, if $\epsilon_3, \ldots, \epsilon_{k-1}$ are expressed as polynomials in δ, then δ_{k-1} is a double zero of all the minors of order 3. The variable transformation (1) preserves the double zero.

The explicit value for δ_{k-1} can be obtained by computing the greatest common divisor of P and P'.

3.2 Characterization of the variable transformation

The condition (5) does not distinguish between the $k-1$ different values for $\delta_1, \ldots, \delta_{k-1}$. We will now establish algebraic conditions between different values $\delta_1, \ldots, \delta_{k-1}$.[3] We will explicitly state these conditions for the cases $k = 5$ and (later on) for $k = 4$. With regard to the security and the computational requirements of the scheme, these seem to be the most interesting cases. The conditions can be established analogously for all $k \geq 6$.

Our aim is to find the matrix A' of the variable transformation. If the variable transformation A' is known, the matrix B' of the linear combinations can be easily computed. We reduce the problem of finding the variable transformation to the problem of finding the coefficients $\delta_1, \ldots, \delta_{k-1}$.

As $\epsilon_3, \ldots, \epsilon_{k-1}$ can be expressed in terms of δ, the matrix associated with

$$v'_1 + \delta v'_2 + \sum_{j=3}^{k-1} \epsilon_j v'_j$$

can be computed in terms of δ. Let Y_i be the row domain of this matrix at δ_i, $1 \leq i \leq k-1$, where $\delta_1, \ldots, \delta_{k-1}$ are defined as in lemma 2. Y_i is a subspace of the vector space $\mathbb{Z}_n^k$. In the following, $\overline{u}_i$ denotes the coefficient vector of the linear function that links in (1) the variable u_i to the variables $y_1, \ldots, y_k$, i.e. $\overline{u}_i := (a_{i1}, \ldots, a_{ik})$, $1 \leq i \leq k$. Each coefficient vector $\overline{u}_i$ is an element of the vector space $\mathbb{Z}_n^k$.

The linear spaces $Y_1, \ldots, Y_{k-1}$ will be characterized by the linear combinations of lemma 2. The vectors $\overline{u}_1, \ldots, \overline{u}_k$ or equivalently the matrix A will be expressed by the linear spaces $Y_1, \ldots, Y_{k-1}$.

[3] Some of the following ideas are due to D.Coppersmith [Co94].

The following fact can easily be checked. Let f, g be linear functions in $y_1, \ldots, y_k$, and let C be the symmetric $k \times k$-matrix associated with the quadratic form $f \cdot g$. The row domain of C is spanned by the coefficient vectors which are canonically associated with the linear functions f and g.

Lemma 3. *For $k = 5$ the linear subspaces $Y_1, \ldots, Y_4$ satisfy*

$$\begin{aligned} Y_1 &= span(\overline{u}_2, \alpha_1\overline{u}_1 + \beta_1\overline{u}_3), \\ Y_2 &= span(\overline{u}_3, \alpha_2\overline{u}_2 + \beta_2\overline{u}_4), \\ Y_3 &= span(\overline{u}_4, \alpha_3\overline{u}_3 + \beta_3\overline{u}_5), \\ Y_4 &= span(\overline{u}_1, \alpha_4\overline{u}_1 + \beta_4\overline{u}_2), \end{aligned}$$

where "span" denotes the set of linear combinations with respect to the vector space $\mathbb{Z}_n^k$.

Proof. The quadratic form of type 1 is $\alpha_1 u_1 u_2 + \beta_1 u_2 u_3 = u_2(\alpha_1 u_1 + \beta_1 u_3)$. Y_i is the matrix that is associated with this quadratic form after applying the variable transformation (1). The statement follows from the fact above. $Y_2, \ldots, Y_4$ can be treated analogously. □

Lemma 4. *The coefficient vectors $\overline{u}_1, \ldots, \overline{u}_5$ satisfy*

$$\begin{aligned} &\overline{u}_1 \in Y_4 \cap (Y_1 + Y_2) && \textit{(dimension 2)}, \\ &\overline{u}_2 \in Y_1 \cap (Y_2 + Y_3) \cap Y_4 && \textit{(dimension 1)}, \\ &\overline{u}_3 \in Y_2 \cap (Y_1 + Y_4) && \textit{(dimension 1)}, \\ &\overline{u}_4 \in Y_3 \cap (Y_2 + Y_1) \cap (Y_2 + Y_4) && \textit{(dimension 1)}, \\ &\overline{u}_5 \in Y_2 + Y_3 && \textit{(dimension 4)}. \end{aligned} \tag{6}$$

Proof. The first statement follows from

$$\begin{aligned} Y_4 \cap (Y_1 + Y_2) &= \operatorname{span}(\overline{u}_1, \alpha_4\overline{u}_1 + \beta_4\overline{u}_2) \\ &\quad \cap \operatorname{span}(\overline{u}_2, \alpha_1\overline{u}_1 + \beta_1\overline{u}_3, \overline{u}_3, \alpha_2\overline{u}_2 + \beta_2\overline{u}_4) \\ &= \operatorname{span}(\overline{u}_1, \overline{u}_2) \cap \operatorname{span}(\overline{u}_1, \overline{u}_2, \overline{u}_3, \overline{u}_4) \\ &= \operatorname{span}(\overline{u}_1, \overline{u}_2), \end{aligned}$$

the other statements can be verified analogously. □

3.3 Computing the variable transformation

So far, we do not know the explicit values for $\delta_1, \delta_2, \delta_3$. Therefore, it is not obvious, whether it is possible to distinguish algebraically between all the subspaces Y_1, Y_2, Y_3. We will show that the spaces Y_1, Y_2, Y_3 or equivalently the values $\delta_1, \delta_2, \delta_3$ are determined uniquely by linear relations. Consequently the values $\delta_1, \delta_2, \delta_3$ are accessible to an algebraic computation. The linear functions $\overline{u}_1, \ldots, \overline{u}_4$ are uniquely determined up to a multiplicative constant. The constants can be chosen arbitrarily, because they can be compensated by the second

private transformation. The condition for $\overline{u}_5$ does not characterize $\overline{u}_5$ uniquely. Due to the explicit computation of δ_4, we already distinguished Y_4 from the set $\{Y_1, Y_2, Y_3\}$.

How to distinguish Y_1 from the set $\{Y_2, Y_3\}$:
It can be easily verified with lemma 3 and 4 that $Y_2 \cap Y_4 = \{0\}$, $Y_3 \cap Y_4 = \{0\}$. From (6) it follows that $\overline{u}_2 \in Y_1 \cap Y_4 \neq \{0\}$. Therefore, the row domain Y_1 can be distinguished from the set $\{Y_2, Y_3\}$.

How to distinguish Y_2 from Y_3:
From the observations $Y_3 \cap (Y_1 + Y_4) = \{0\}$, $\overline{u}_3 \in Y_2 \cap (Y_1 + Y_4) \neq \{0\}$, the linear spaces Y_2 and Y_3 can be distinguished.

As the intersections for $\overline{u}_2$, $\overline{u}_3$, $\overline{u}_4$ in (6) are of dimension 1, these coefficient vectors are uniquely determined up to a multiplicative constant.

How to determine $\overline{u}_1$ uniquely:
The intersection $Y_4 \cap (Y_1 + Y_2)$ is of dimension 2. From (6) it follows that $\overline{u_1}$ and $\overline{u_2}$ are elements of this intersection, i.e. $Y_4 \cap (Y_1 + Y_2) = \operatorname{span}(\overline{u_1}, \overline{u_2})$. The division of the quadratic form $u_2(\alpha_1 u_1 + \beta_1 u_3)$ by the linear form u_2 yields the linear form $\alpha_1 u_1 + \beta_1 u_3$. We observe that $\overline{u}_1$ satisfies the condition

$$\overline{u}_1 \in \operatorname{span}(\overline{u}_3, \alpha_1 \overline{u}_1 + \beta_1 \overline{u}_3),$$

whereas a linear combination $a \cdot \overline{u}_1 + b \cdot \overline{u}_2$ with $b \neq 0$ does not satisfy the condition. This condition serves to distinguish $\overline{u_1}$ among the space $\operatorname{span}(\overline{u_1}, \overline{u_2})$. Consequently, $\overline{u}_1$ is uniquely determined.

How to determine $\overline{u}_5$:
For $\overline{u}'_5 = a\overline{u}_3 + b\overline{u}_5 \in \operatorname{span}(\overline{u}_3, \overline{u}_5)$ and a variable u'_5 linked to the variables $y_1, \ldots, y_5$ via the coefficient vector $\overline{u}'_5$, it follows

$$\begin{aligned} &a_1 \cdot u_1^2 + a_2 \cdot u_1 u_2 + a_3 \cdot u_2 u_3 + a_4 \cdot u_3 u_4 + a_5 \cdot u_4 u'_5 \\ &= a_1 \cdot u_1^2 + a_2 \cdot u_1 u_2 + a_3 \cdot u_2 u_3 + (a_4 + a\, a_5) \cdot u_3 u_4 + b\, a_5 \cdot u_4 u_5, \end{aligned}$$

i.e. every linear combination of $u_1^2, \ldots, u_4 u_5$ is a linear combination of $u_1^2, \ldots, u_3 u_4$, $u_4 u'_5$ and vice versa. Therefore, $\overline{u}_5$ is not determined uniquely. However, it can be replaced by an element $\overline{u}'_5$ in $\operatorname{span}(\overline{u}_3, \overline{u}_5)$ without changing the space of the linear combinations. Such an element can be obtained by dividing the quadratic form $u_4 \cdot (\alpha_3 u_3 + \beta_3 u_5)$ by u_4.

The process of distinguishing the subspaces Y_1, Y_2, Y_3 and the coefficient vectors $\overline{u}_1, \ldots, \overline{u}_5$ can be effectively done with algebraic standard methods, especially determinants and resultants. Of course, the realization of the algebraic condition will lead to high degree polynomials in the variables $\delta_1, \delta_2, \delta_3$. For technical and practical reasons the polynomials have to be reduced. Fortunately, due to the polynomial equation $P(\delta) = 0$ of degree 5, all polynomials can be reduced to degree 4 in each variable. When the double zero δ_4 has been computed, the polynomial $Q(\delta) := P(\delta)/(\delta - \delta_4)^2$ is of degree 3 and serves to reduce

each polynomial to degree 4 in each variable. In fact, as $\delta_1, \ldots, \delta_4$ are pairwise different, the polynomials can even be reduced much better.

The ability to distinguish between the subspaces Y_1, Y_2, Y_3 means that we can also compute explicit values for $\delta_1, \delta_2, \delta_3$. These values can be used to evaluate the polynomial expressions for $\overline{u}_1, \ldots, \overline{u}_4, \overline{u}'_5$. The matrix A' that is formed by the rows $\overline{u}_1, \ldots, \overline{u}_4, \overline{u}'_5$ can replace the variable transformation from (1). The missing fifth polynomial can be replaced by the quadratic form

$$\overline{v}_5 := u_1^2 + \sum_{i=1}^{3} u_i u_{i+1} + u_4 u'_5.$$

By inverting the matrix A', the polynomials $v'_1, \ldots, v'_4, \overline{v}_5$ become polynomials in terms of $u_1, \ldots, u_5$. These polynomials are linear combinations of the basis elements and define a matrix B' according to (2). The pair of matrices (A', B') generates the given public key. Therefore we have found the secret key.

3.4 The case $k = 4$

We will now explain the modifications to the case $k = 5$ that are necessary to obtain an attack for $k = 4$. Most of the considerations are identical. It remains to show that all the spaces of Y_1, Y_2, Y_3 or equivalently $\delta_1, \delta_2, \delta_3$ can be distinguished.

When $k = 4$, the quadratic forms of a rank not greater than 2 are of the form

$$\begin{array}{rll} & \alpha_1 u_1 u_2 + \beta_1 u_2 u_3 & \text{(type 1)}, \\ & \alpha_2 u_2 u_3 + \beta_2 u_3 u_4 & \text{(type 2)}, \\ \text{or} & \alpha_3 u_1^2 + \beta_3 u_1 u_2 & \text{(type 3)}. \end{array}$$

With respect to the sum

$$v_1 + \delta v_2 + \epsilon_3 v_3,$$

the condition of type i defines δ_i, $1 \leq i \leq 3$. We obtain a polynomial $P(\delta)$ of degree 4. The double zero δ_3 can be extracted by computing the greatest common divisor of P and P'. The following two lemmas can be verified like in the case $k = 5$

Lemma 5. *For $k = 4$ the linear subspaces Y_1, Y_2, Y_3 satisfy*

$$\begin{aligned} Y_1 &= span(\overline{u}_2, \alpha_1 \overline{u}_1 + \beta_1 \overline{u}_3), \\ Y_2 &= span(\overline{u}_3, \alpha_2 \overline{u}_2 + \beta_2 \overline{u}_4), \\ Y_3 &= span(\overline{u}_1, \alpha_3 \overline{u}_1 + \beta_3 \overline{u}_2). \end{aligned}$$

Lemma 6. *For $k = 4$ the coefficient vectors $\overline{u}_1, \ldots, \overline{u}_4$ satisfy*

$$\begin{array}{ll} \overline{u}_1 \in Y_3 \cap (Y_1 + Y_2) & \textit{(dimension 2)}, \\ \overline{u}_2 \in Y_1 \cap Y_3 & \textit{(dimension 1)}, \\ \overline{u}_3 \in Y_2 \cap (Y_1 + Y_3) & \textit{(dimension 1)}, \\ \overline{u}_4 \in Y_2 + Y_3 & \textit{(dimension 4)}. \end{array}$$

δ_3 and therefore Y_3 is already known. Y_1 and Y_2 can be distinguished because of $\overline{u}_2 \in Y_1 \cap Y_3 \neq \{0\}$, $Y_2 \cap Y_3 = \{0\}$.

$\overline{u}_2$ and $\overline{u}_3$ are characterized by one-dimensional spaces. $\overline{u}_1$ can be distinguished from $\overline{u}_2$ in the same way as for $k = 5$. $\overline{u}_4$ can be replaced by the element $\overline{u}'_4 = \alpha_2\overline{u}_2 + \beta_2\overline{u}_4$. We further proceed like in the case $k = 5$.

3.5 Composite moduli

If n is a composite modulus of the form $p \cdot q$, there are $k^2 = 25$ zeros of the polynomial $P(\delta)$ modulo n. Both modulo p and modulo q, δ_{k-1} is a double zero. The sequence $\delta_1, \ldots, \delta_{k-1}$ is unique modulo p, and it is unique modulo q. Although there are $(k-1)^2$ different zeros of the polynomial modulo n, only one sequence $\delta_1, \ldots, \delta_{k-1}$ satisfies the uniqueness modulo p and modulo q. Therefore the Chinese remainder theorem guarantees that all computations work in the case of a composite modulus.

3.6 Experimental results

We implemented the attack for moderate key sizes of 50 bits using the package MATHEMATICA. The implementation breaks a given public key within 15 minutes on a HP workstation 735/50, although we did not aim at optimizing the program. For a larger modulus, the number of main steps in the attack does *not* increase. Of course, the cost of the elementary operations like polynomial addition and multiplication increase with the length of the modulus.

The recommended bit length for the modulus in [Sh93b] is 512. We estimate that an implementation for this key size runs in at most a few hours. Further details of an implementation as well as an example of the computation can be found in [The95].

4 Symmetric basis versus asymmetric basis

There are some remarkable differences between the attack on the symmetric basis $\{u_1u_2, \ldots, u_{k-1}u_k, u_ku_1\}$ in [CSV93] and our attack on the asymmetric basis. These differences lead to a better insight into the attacks. In the symmetric case, there are several equivalent sequences for the coefficients $\delta_1, \ldots, \delta_k$. Therefore these coefficients cannot be computed. The sequence $\delta_1, \ldots, \delta_{k-1}$ is unique in the asymmetric case. Lemma 4 and 6 provide the necessary conditions to distinguish among the coefficients $\delta_1, \ldots, \delta_{k-1}$. All coefficients can be computed, and it is possible to discover the secret key.

Considering a composite modulus in the symmetric case, each (unknown) sequence of the coefficients modulo p can be combined with each (unknown) sequence of the coefficients modulo q. This is the essential reason why the computation of the secret key is at least as hard as factoring the modulus (see [Sh93b]). For the asymmetric basis, the sequence of the coefficients is unique even modulo

n. Our attack therefore shows that the asymmetric basis does not fit into the framework of difficult algebraic instances that was developed in [Sh93a].

From a practical point of view, we can mention the following results: Due to the ability to compute $\delta_1, \ldots, \delta_{k-1}$, the attack on the asymmetric basis can get rid of the time-consuming large polynomials. Therefore it takes much less time to attack the asymmetric basis than to attack the symmetric basis.

5 Open questions

The intention of [CSV93] and of our work was to break some specific proposed cryptosystems. For further research in the cryptographic applications of polynomials, it would be of interest to characterize the power of these cryptanalytic methods from a more general point of view. In a cryptosystem that is resistant against the presented cryptanalytic methods, the trapdoor condition should *not* influence the rank of quadratic forms. Otherwise, this influence is a promising starting point for an attack.

Acknowledgements

I wish to thank D. Coppersmith, C. P. Schnorr and S. Vaudenay for their encouragement and support.

References

[Co94] D. Coppersmith: Private communication (1994).

[CSV93] D. Coppersmith, J. Stern and S. Vaudenay: Attacks on the Birational Permutation Signature Schemes. Proceedings of CRYPTO 93, Lecture Notes in Computer Science 773, 435-443 (1993).

[Ja74] N. Jacobson: Basic Algebra. W. H. Freeman and Company, San Francisco (1974).

[Mi93] B. Mishra: Algorithmic Algebra. Springer-Verlag, New York (1993).

[Na93] D. Naccache: Can O.S.S. be Repaired ? - Proposal for a New Practical Signature Scheme. Proceedings of Eurocrypt 93, Lecture Notes in Computer Science 765, 233-239 (1993).

[OSS84] H. Ong, C. P. Schnorr, A. Shamir: A Fast Signature Scheme Based on Quadratic Equations. Proceedings 16th ACM Symposium on Theory of Computing, 208-216 (1984).

[PS87] J. M. Pollard, C. P. Schnorr: An Efficient Solution to the Congruence $x^2 + y^2 = m \pmod{n}$. IEEE Transactions on Information Theory, Vol. 33, 702-709 (1987).

[Sh93a] A. Shamir: On the Generation of Multivariate Polynomials Which Are Hard To Factor. Proceedings 25th ACM Symposium on Theory of Computing, 796-804 (1993).

[Sh93b] A. Shamir: Efficient Signature Schemes Based on Birational Permutations. Proceedings of CRYPTO 93, Lecture Notes in Computer Science 773, 1-12 (1993).

[The95] T. Theobald: Digitale Unterschriften mittels birationaler Permutationen. Diplomarbeit, Universität Frankfurt (1995).

Appendix: Proof of Lemma 1

Proof. Let

$$a_1 u_1^2 + \sum_{i=2}^{k} a_i\, u_{i-1} u_i, \quad a_1, \ldots, a_k \in \mathbb{Z}_n \tag{7}$$

be a linear combination of the basis elements and Q the associated matrix. The matrix Q is (for better clearness zero-entries are omitted)

$$Q = \frac{1}{2} \begin{pmatrix} 2a_1 & a_2 & & & & \\ a_2 & & a_3 & & & \\ & a_3 & & a_4 & & \\ & & a_4 & & \ddots & \\ & & & \ddots & & a_k \\ & & & & a_k & \end{pmatrix}.$$

"$\Longleftarrow$" Obviously, a linear combination (7) of type $t \in \{1, \ldots, k-1\}$ is of rank not greater than 2.
"$\Longrightarrow$" We assume, that the linear combination (7) is not of the form (3).
Case 1: $a_1 = 0$. It follows

$$Q = \frac{1}{2} \begin{pmatrix} 0 & a_2 & & & & \\ a_2 & & a_3 & & & \\ & a_3 & & a_4 & & \\ & & a_4 & & \ddots & \\ & & & \ddots & & a_k \\ & & & & a_k & \end{pmatrix}.$$

For $j := \min\{i \in \{2, \ldots, k\} : a_i \neq 0\}$ and $l := \max\{i \in \{2, \ldots, k\} : a_i \neq 0\}$, we have $l - j \geq 2$. The 3×3-submatrix

$$\frac{1}{2} \begin{pmatrix} 0 & a_j & 0 \\ a_j & 0 & x \\ 0 & 0 & a_l \end{pmatrix} \quad \text{with } x := \begin{cases} 0, & \text{if } l - j > 2 \\ a_{j+1}, & \text{if } l - j = 2 \end{cases}$$

of Q has determinant $-(\frac{1}{2})^3 a_j^2 a_l \neq 0$. Therefore rank $Q \geq 3$.

Case 2: $a_1 \neq 0$. For $j := \min\{i \in \{3, \ldots, k\} : a_i \neq 0\}$ the upper left $j \times j$-submatrix of Q is

$$\frac{1}{2}\begin{pmatrix} 2a_1 & a_2 & & & & \\ a_2 & 0 & & & & \\ & & 0 & & \ddots & \\ & & & \ddots & & 0 \\ & & & & 0 & a_j \\ & & & & a_j & \end{pmatrix}.$$

The 3×3-submatrix

$$\frac{1}{2}\begin{pmatrix} 2a_1 & x & 0 \\ x & 0 & a_j \\ 0 & a_j & 0 \end{pmatrix} \quad \text{with } x := \begin{cases} 0, & \text{if } j > 3 \\ a_2, & \text{if } j = 3 \end{cases}$$

has determinant $-(\frac{1}{2})^2 a_1 a_j^2 \neq 0$. It follows rank $Q \geq 3$. □