Further Attacks on the Birational Permutation Signature Schemes

Thorsten Theobald
Fachbereich Mathematik/Informatik, AG 7.2, Universität Frankfurt,
Robert-Mayer-Strasse 6-10, 60054 Frankfurt a. M., Germany
e-mail: theobald@informatik.uni-frankfurt.de

October 21, 1994

Abstract

At Crypto 93, Shamir [3] proposed two signature schemes based on birational permutations. Coppersmith, Stern and Vaudenay [2] presented the first attacks on both cryptosystems. These attacks do not recover the secret key. For one of the variants proposed by Shamir we show how to recover the secret key.

1 Introduction and history

A low degree rational mapping whose inverse is also a low degree rational mapping is called a birational permutation. Shamir [3] used this concept to introduce signature schemes with low computational requirements. Both the generation and the verification of the signatures can be done with very few modular multiplications.

The second of these schemes depends on the choice of an algebraic basis. Shamir proposed two bases: a symmetric one and an asymmetric one. The attack of Coppersmith et al. [2] concentrates on the symmetric basis. It is possible to forge signatures, but the secret key is not revealed. Here we show how to attack the asymmetric basis. In this case, it is even possible to discover the secret key.

2 The signature scheme

Let n be the product of two large secret primes p and q. All computations will be done in $\mathbb{Z}_n$. Consider the set of polynomials $G = \{u_1^2, u_1u_2, u_2u_3, \ldots, u_{k-1}u_k\}$. As explained in [3], the set G has the property of an algebraic basis. Therefore every assignment of a vector $x \in \mathbb{Z}_n^k$ to the elements of G implies unique assignments to all homogeneous polynomials of degree 2 in $u_1, \ldots, u_k$. We call G the asymmetric basis.

Two secret linear transformations A and B are used to mix up the polynomials: the variable transformation

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

and the linear combinations

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

The polynomials $v_1, \ldots, v_k$ in the new variables $y_1, \ldots, y_k$ can be written in the form

$$v_i = \sum_{j,l} (C_i)_{j,l}\, y_j y_l, \quad C_i \text{ symmetric}, \quad 1 \leq i \leq k.$$

The public key consists of the matrices $C_1, \ldots, C_{k-1}$. C_k is not published in order to prevent unique signatures.

Each message m is represented by $k-1$ hash values $h_1(m), \ldots, h_{k-1}(m)$. An assignment to the basis elements $y_1^2, y_1 y_2, \ldots, y_{k-1} y_k$ is a valid signature for m if and only if

$$\sum_{j,l} (C_i)_{j,l}\, y_j y_l = h_i(m), \quad 1 \leq i \leq k-1.$$

3 The attack

The general idea of the attack is to find algebraic conditions for the rank of quadratic forms. Such statements about the rank are invariants with respect to the variable transformation.

We first consider $k = 5$ and then $k = 4$. With regard to the security and the computational requirements of the scheme, these seem to be the the most interesting cases.

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.

3.1 The structure of the representation matrices

We examine linear combinations of the basis elements $u_1^2, u_1 u_2, \ldots, u_4 u_5$. The corresponding representation matrix is of the following form (a star represents an arbitrary entry):

$$\begin{pmatrix} \star & \star & 0 & 0 & 0 \\ \star & 0 & \star & 0 & 0 \\ 0 & \star & 0 & \star & 0 \\ 0 & 0 & \star & 0 & \star \\ 0 & 0 & 0 & \star & 0 \end{pmatrix}$$

The matrix has relatively few non-zero entries. A careful inspection of its structure leads to the following

Lemma 3.1 The linear combinations which are quadratic forms of a rank not greater than 2 are of the form

$$\begin{array}{rll} & \alpha_1 u_1 u_2 + \beta_1 u_2 u_3 & \text{(type 1)}, \\ & \alpha_2 u_2 u_3 + \beta_2 u_3 u_4 & \text{(type 2)}, \\ & \alpha_3 u_3 u_4 + \beta_3 u_4 u_5 & \text{(type 3)}, \\ \text{or} & \alpha_4 u_1^2 + \beta_4 u_1 u_2 & \text{(type 4)} \end{array}$$

with coefficients $\alpha_i, \beta_i \in \mathbb{Z}_n$.

The coefficients of the basis elements form a vectorspace of dimension 5. For each $i \in \{1, \ldots, 4\}$ the pair (α_i, β_i) describes a twodimensional subspace. Now we consider

$$v_1 + \delta v_2 + \epsilon_3 v_3 + \epsilon_4 v_4.$$

In the original variables $u_1, \ldots, u_5$, this sum also describes a linear combination of the basis elements $u_1^2, u_1 u_2, \ldots, u_{k-1} u_k$. The subspace that is formed by δ, ϵ_3 and ϵ_4 is of dimension 3. This specifies some intersections which consist of only one element.

Lemma 3.2 For each $i \in \{1, \ldots, 4\}$ there exists exactly one pair $(\alpha_i, \beta_i) \in \mathbb{Z}_n^2$ and exactly one triple $(\delta, \epsilon_3, \epsilon_4) \in \mathbb{Z}_n^3$, such that the quadratic forms of type i can be represented by the linear combination

$$v_1 + \delta v_2 + \epsilon_3 v_3 + \epsilon_4 v_4,$$

i.e.

$$\begin{array}{lll} \exists_1 (\alpha_1, \beta_1) & \exists_1 (\delta_1, \epsilon_{3,1}, \epsilon_{4,1}) & \alpha_1 u_1 u_2 + \beta_1 u_2 u_3 = v_1 + \delta_1 v_2 + \epsilon_{3,1} v_3 + \epsilon_{4,1} v_4, \\ \exists_1 (\alpha_2, \beta_2) & \exists_1 (\delta_2, \epsilon_{3,2}, \epsilon_{4,2}) & \alpha_2 u_2 u_3 + \beta_2 u_3 u_4 = v_1 + \delta_2 v_2 + \epsilon_{3,2} v_3 + \epsilon_{4,2} v_4, \\ \exists_1 (\alpha_3, \beta_3) & \exists_1 (\delta_3, \epsilon_{3,3}, \epsilon_{4,3}) & \alpha_3 u_3 u_4 + \beta_3 u_4 u_5 = v_1 + \delta_3 v_2 + \epsilon_{3,3} v_3 + \epsilon_{4,3} v_4, \\ \exists_1 (\alpha_4, \beta_4) & \exists_1 (\delta_4, \epsilon_{3,4}, \epsilon_{4,4}) & \alpha_4 u_1^2 + \beta_4 u_1 u_2 = v_1 + \delta_4 v_2 + \epsilon_{3,4} v_3 + \epsilon_{4,4} v_4. \end{array}$$

A symmetric $k \times k$-matrix has

$$\frac{1}{2}\binom{5}{3}\binom{5}{3} + \frac{1}{2}\binom{5}{3} = 55$$

different minors of order 3. The minors are used to express ϵ_3 and ϵ_4 in terms of δ. Furthermore, we find a polynomial $P(\delta)$ with roots $\delta_1, \ldots, \delta_4$. The representation matrix corresponding to the quadratic form of type 4 is

$$\begin{pmatrix} \star & \star & 0 & 0 & 0 \\ \star & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Each submatrix of order 3 consists of at least one row and one column in which only zeros appear. Therefore δ_4 is a double zero of $P(\delta)$. The polynomial $P(\delta)$ is of degree 5. δ_4 can be extracted by computing the greatest common divisor of P and P'.

Technical Details

Each minor of order 3 generates a polynomial equation of the form

$$\sum_{0 \le i,j,l \le 3,\ i+j+l \le 3} \lambda_{ijl} \cdot \delta^i \epsilon_3^j \epsilon_4^l = 0$$

with coefficients $\lambda_{ijl} \in \mathbb{Z}_n$, $1 \le i, j, l \le 5$. Using an idea of S. Vaudenay [4], each term $\delta^i \epsilon_3^j \epsilon_4^l$ can be considered as an unknown in a system of linear equations. Analogous to the Gaussian elimination algorithm, the terms are successively removed. At the end, we obtain an expression for ϵ_3 in terms of ϵ_4, δ. By applying the method once again, we find an expression for ϵ_4 in terms of δ. After the substitution of ϵ_3 and ϵ_4, we continue and obtain a polynomial in δ of degree 5.

3.2 Characterization of the variable transformation

The representation matrix of

$$v_1 + \delta v_2 + \epsilon_3 v_3 + \epsilon_4 v_4$$

can be computed in terms of δ. Let Y_i be the row domain of the representation matrix at δ_i, $1 \le i \le 4$. In the following, u_i also denotes the coefficient vector of the linear function that links the variable u_i to the variables y_j.

For the characterization of the variable transformation, the following fact is used: Let f, g be linear functions in $y_1, \ldots, y_k$, and let C be the symmetric $k \times k$-matrix of the quadratic form $f \cdot g$. The row domain of C is spanned by the coefficient vectors which describe the linear functions f and g.

Lemma 3.3 It holds

$$\begin{array}{rcl} Y_1 & = & \operatorname{span}(u_2, \alpha_1 u_1 + \beta_1 u_3), \\ Y_2 & = & \operatorname{span}(u_3, \alpha_2 u_2 + \beta_2 u_4), \\ Y_3 & = & \operatorname{span}(u_4, \alpha_3 u_3 + \beta_3 u_5), \\ Y_4 & = & \operatorname{span}(u_1, \alpha_4 u_1 + \beta_4 u_2). \end{array}$$

The coefficient vectors $u_1, \ldots, u_5$ can be characterized by the row domains $Y_1, \ldots, Y_5$.

Lemma 3.4 It holds

$$\begin{array}{rcll} u_1 & \in & Y_4 \cap (Y_1 + Y_2) & \text{(dimension 2)}, \\ u_2 & \in & Y_1 \cap (Y_2 + Y_3) \cap Y_4 & \text{(dimension 1)}, \\ u_3 & \in & Y_2 \cap (Y_1 + Y_4) & \text{(dimension 1)}, \\ u_4 & \in & Y_3 \cap (Y_2 + Y_1) \cap (Y_2 + Y_4) & \text{(dimension 1)}, \\ u_5 & \in & Y_2 + Y_3 & \text{(dimension 4)}. \end{array}$$

3.3 Reducing the polynomials

The realization of the algebraic conditions will lead to high degree polynomials in several variables. The following method can be used to reduce the polynomials. Let $Q(\delta)$ be the polynomial whose zeros are δ_1, δ_2 and δ_3. Each occurence of a variable δ_i can be reduced to degree 2 by subtracting multiples of $Q(\delta_i)$, $1 \le i \le 3$.

To assure that δ_1, δ_2 and δ_3 are different solutions of $Q(\delta)$, we define

$$\begin{array}{rcl} Q_2(\delta) & = & \dfrac{Q(\delta) - Q(\delta_1)}{\delta - \delta_1}, \\ Q_3(\delta) & = & \dfrac{Q_2(\delta) - Q_2(\delta_2)}{\delta - \delta_2}. \end{array}$$

It holds

$$Q_2(\delta_2) = 0, \quad Q_2(\delta_3) = 0, \quad Q_3(\delta_3) = 0.$$

$Q_2(\delta_2)$ is of degree 2 in δ_2, $Q_3(\delta_3)$ is of degree 1 in δ_3. Therefore each occurence of δ_2 can be reduced to degree 1. Each occurence of δ_3 can be eliminated.

3.4 Successive computation of the variable transformation

Some of the following ideas are due to D. Coppersmith [1].

The linear functions $u_1, \ldots, u_4$ 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 u_5 does not characterize u_5 uniquely.

Lemma 3.5 u_2 is the only coefficient vector in the intersection of a subspace Y_i, $1 \leq i \leq 3$, with Y_4, namely $u_2 \in Y_1 \cap Y_4$. This relation serves to determine δ_1 uniquely. δ_1 can be computed.

Proof It holds $Y_2 \cap Y_4 = \emptyset$, $Y_3 \cap Y_4 = \emptyset$. The intersection $Y_1 \cap (Y_2 + Y_3)$ is of dimension 1 and yields a polynomial expression for u_2. The relation $u_2 \in Y_4$ can be used to establish a polynomial equation. δ_1 is the only element, which satisfies both this equation and the equation $Q(\delta) = 0$. With the aid of resultants, δ_2 can be eliminated from the system of equations. This leads to a quadratic equation in δ_1. By computing the greatest common divisor of the quadratic polynomial and $Q(\delta_1)$ in $\mathbb{Z}_n$, we obtain the explicite value for δ_1. □

As δ_1 is known, the polynomial $Q(\delta)$ of degree 3 can be transformed into a polynomial $R(\delta)$ of degree 2. Define

$$R_2(\delta) = \frac{R(\delta) - R(\delta_2)}{\delta - \delta_2}$$

It holds $R_2(\delta_3) = 0$. $R_2(\delta_3)$ is of degree 1 in δ_3. In arbitrary polynomial equations, each occurence of δ_2 can be reduced to degree 1. Each occurence of δ_3 can be eliminated.

Lemma 3.6 u_3 is the only coefficient vector, which is in an intersection of a subspace Y_i, $2 \leq i \leq 3$, with $(Y_1 + Y_4)$. It holds $u_3 \in Y_2 \cap (Y_1 + Y_4)$. With this relation δ_2 is determined uniquely, and it can be computed.

Proof The intersection $Y_3 \cap (Y_1 + Y_4)$ is empty. Therefore the intersection $Y_i \cap (Y_1 + Y_4)$ distinguishes δ_2 and δ_3. This yields a polynomial relation for u_3 and an equation for δ_2 which is not satisfied by δ_3. The equation can be reduced. We obtain a linear equation in δ_2, which can be solved. □

As δ_1, δ_2 and δ_4 are known, we also obtain the value for δ_3. It is no longer necessary to compute in residue class rings modulo polynomials in δ_i. The following computations can be done in $\mathbb{Z}_n$.

Lemma 3.7 u_4 is the only coefficient vector in the intersection $Y_3 \cap (Y_2 + Y_1)$.

Proof The intersection $Y_3 \cap (Y_2 + Y_1)$ is of dimension 1 and produces an equation for u_4. □

Lemma 3.8 The relation $u_1 \in Y_4 \cap (Y_1 + Y_2)$ and the quadratic form $u_2 \cdot (\alpha_1 u_1 + \beta_1 u_3)$ can be used to compute u_1.

Proof The intersection $Y_4 \cap (Y_1 + Y_2)$ is of dimension 2. Not only u_1 is an element of this intersection, but also u_2. The representation matrix of the linear combination at δ_1 corresponds to the quadratic form $u_2 \cdot (\alpha_1 u_1 + \beta_1 u_3)$. We divide the quadratic form by the explicitely known linear form u_2 and obtain the linear function $\alpha_1 u_1 + \beta_1 u_3$. Using the fact, that u_1 satisfies the condition

$$u_1 \in \operatorname{span}(u_3, \alpha_1 u_1 + \beta_1 u_3),$$

u_1 and u_2 can be distinguished. A linear combination $a \cdot u_1 + b \cdot u_2$ with $b \neq 0$ does not satisfy the condition. Therefore u_1 is characterized uniquely. □

Lemma 3.9 u_5 is not determined uniquely, but it can be replaced by an element u_5' in $\operatorname{span}(u_3, u_5)$. Such an element can be obtained by considering the quadratic form $u_4 \cdot (\alpha_3 u_3 + \beta_3 u_5)$.

Proof The division of the known quadratic form $u_4 \cdot (\alpha_3 u_3 + \beta_3 u_5)$ by u_4 yields

$$u_5' = \alpha_3 u_3 + \beta_3 u_5.$$

Each 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, because

$$\begin{aligned} & a_1 \cdot u_1^2 + a_2 \cdot u_1 u_2 + a_3 \cdot u_2 u_3 + a_4 \cdot u_3 u_4 + a_5 \cdot u_4 u_5' \\ = \; & a_1 \cdot u_1^2 + a_2 \cdot u_1 u_2 + a_3 \cdot u_2 u_3 + (a_4 + \alpha_3 a_5) \cdot u_3 u_4 + \beta_3 a_5 \cdot u_4 u_5. \end{aligned}$$

□

The matrix A' that is formed by the rows $u_1, \ldots, u_4$, u_5' can replace the variable transformation A. The missing fifth equation, can be established by computing

$$v_5' = u_1^2 + \sum_{i=1}^{3} u_i u_{i+1} + u_4 u_5'.$$

By inverting the matrix A', we can express the polynomials $v_1, \ldots, v_4, v_5'$ in terms of $u_1, \ldots, u_5$. These polynomials are linear combinations of the basis elements. They describe a representative B' for the secret matrix B. The pair of matrices (A', B') generates the same public key as the pair (A, B). Therefore we have found the secret key.

3.5 Composite moduli

If n is a composite modulus of the form $p{\cdot}q$, there are $5^2 = 25$ zeros of the polynomial $P(\delta)$ modulo n. Both modulo p and modulo q, δ_4 is a double zero. The sequence $\delta_1, \ldots, \delta_4$ is unique modulo p, and it is unique modulo q. Although there are $4{\cdot}4 = 16$ different zeros of the polynomial modulo n, only one sequence $\delta_1, \ldots, \delta_4$ satisfies the uniqueness modulo p and modulo q. Therefore the chinese remaindering theorem guarantees that all computations work in the case of a composite modulus.

3.6 Example

In order to present a reasonable example without too big numbers, we choose the prime modulus $n = 7853$. The example was computed on a HP workstation 9000, model 735/50 within 15 minutes. The implementation uses the package MATHEMATICA.

The numerical data of the example can be found in the appendix.

3.7 The case $k = 4$

In case of the symmetric basis $\{u_1u_2, u_2u_3, \ldots, u_ku_1\}$, k has to be odd. When using the asymmetric basis, it is possible to choose $k = 4$. 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 values of $\delta_1, \ldots, \delta_4$ can be distinguished.

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

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

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 divisior of P and P'.

Lemma 3.10 It holds

$$\begin{aligned} Y_1 &= \operatorname{span}(u_2, \alpha_1 u_1 + \beta_1 u_3), \\ Y_2 &= \operatorname{span}(u_3, \alpha_2 u_2 + \beta_2 u_4), \\ Y_3 &= \operatorname{span}(u_1, \alpha_3 u_1 + \beta_3 u_2). \end{aligned}$$

Lemma 3.11 The conditions for characterizing $u_1, \dots, u_4$ are

$$\begin{array}{lcll} u_1 & \in & Y_3 \cap (Y_1 + Y_2) & \text{(dimension 2)}, \\ u_2 & \in & Y_1 \cap Y_3 & \text{(dimension 1)}, \\ u_3 & \in & Y_2 \cap (Y_1 + Y_3) & \text{(dimension 1)}, \\ u_4 & \in & Y_2 + Y_3 & \text{(dimension 4)}. \end{array}$$

δ_3 and therefore Y_3 is known. u_2 and δ_1 are characterized by

$$u_2 \in Y_1 \cap Y_3.$$

When δ_1 has been computed, the remaining zero of $P(\delta)$ is δ_2.

u_1 und u_3 can be computed analogous to the case $k = 5$. u_4 can be replaced by the element

$$u'_4 = \alpha_2 u_2 + \beta_2 u_4.$$

We further proceed like in the case $k = 5$.

4 Symmetric basis versus asymmetric basis

There are some remarkable differences between the attacks on the symmetric and the asymmetric basis. In the symmetric case, there are several equivalent sequences for the δ_i. Therefore the δ_i and the secret key cannot be computed. The sequence of the δ_i is unique in the asymmetric case. All δ_i 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 δ_i modulo p can be combined with each (unknown) sequence of the δ_i modulo q. For the asymmetric basis, the sequence of the δ_i is unique even modulo n.

From a practical point of view, we can mention the following results: Due to the ability to compute the δ_i, the attack on the asymmetric basis can get rid of the time-consuming large polynomials. Therefore it takes less time to attack the asymmetric basis than to attack the symmetric basis.

With regard to other cryptographic applications and to general polynomial equations, it seems to be quite interesting what a little symmetry can cause.

Acknowledgements

I wish to thank D. Coppersmith, C. P. Schnorr and S. Vaudenay. Without their encouragement and support this work would have not been created.

References

[1] D. Coppersmith: Private communication, 1994.

[2] D. Coppersmith, J. Stern and S. Vaudenay: Attacks on the Birational Permutation Signature Schemes, Proceedings of CRYPTO 93, LNCS 773, pp. 435-443.

[3] A. Shamir: Efficient Signature Schemes Based on Birational Permutations, Proceedings of CRYPTO 93, LNCS 773, pp. 1-12.

[4] S. Vaudenay: Private communication, 1994.

Appendix

Example for k = 5

The modulus n is 7853. The transformation matrices are

$$A = \begin{pmatrix} 936 & 75 & 494 & 559 & 229 \\ 70 & 868 & 624 & 42 & 975 \\ 855 & 568 & 573 & 532 & 227 \\ 670 & 96 & 705 & 225 & 5 \\ 724 & 437 & 247 & 928 & 818 \end{pmatrix}, \quad B = \begin{pmatrix} 684 & 53 & 821 & 512 & 509 \\ 951 & 651 & 172 & 252 & 776 \\ 468 & 610 & 618 & 892 & 293 \\ 476 & 300 & 750 & 899 & 126 \\ 365 & 404 & 502 & 863 & 190 \end{pmatrix}.$$

The vector (C_1, C_2, C_3, C_4) of the public key matrices is

$$\left(\begin{pmatrix} 2153 & 6906 & 5444 & 4821 & 4167 \\ 6906 & 2217 & 3423 & 2726 & 5159 \\ 5444 & 3423 & 1306 & 839 & 4933 \\ 4821 & 2726 & 839 & 3565 & 959 \\ 4167 & 5159 & 4933 & 959 & 2118 \end{pmatrix}, \begin{pmatrix} 6787 & 171 & 3691 & 7801 & 3328 \\ 171 & 4748 & 6402 & 1723 & 7382 \\ 3691 & 6402 & 2652 & 1987 & 4808 \\ 7801 & 1723 & 1987 & 374 & 6905 \\ 3328 & 7382 & 4808 & 6905 & 6785 \end{pmatrix}, \begin{pmatrix} 3087 & 6028 & 7727 & 5383 & 4720 \\ 6028 & 7747 & 4963 & 251 & 5766 \\ 7727 & 4963 & 655 & 7536 & 1080 \\ 5383 & 251 & 7536 & 1957 & 1933 \\ 4720 & 5766 & 1080 & 1933 & 4327 \end{pmatrix}, \begin{pmatrix} 3974 & 1655 & 6643 & 1028 & 6987 \\ 1655 & 3987 & 5379 & 4330 & 1815 \\ 6643 & 5379 & 1466 & 3502 & 1609 \\ 1028 & 4330 & 3502 & 5984 & 7264 \\ 6987 & 1815 & 1609 & 7264 & 2898 \end{pmatrix} \right).$$

We obtain the following relation for ϵ_3 in terms of ϵ_4, δ:

$$\epsilon_3 = 4114 + 5969\delta + 1868\delta^2 + 4890\delta^3 + 2525\epsilon_4.$$

The relation for ϵ_4 in terms of δ is

$$\epsilon_4 = 2087 + 1257\delta + 7850\delta^2 + 1152\delta^3 + 755\delta^4.$$

Using the polynomial $P(\delta)$, δ_4 can be computed.

$$\begin{aligned} P(\delta) &= 6893 + 865\delta + 3240\delta^2 + 3987\delta^3 + 4768\delta^4 + \delta^5, \\ P'(\delta) &= 865 + 6480\delta + 4108\delta^2 + 3366\delta^3 + 5\delta^4, \\ \gcd(P, P') &= \delta - 4950. \end{aligned}$$

It follows $\delta_4 = 4950$.

The remaining polynomial of degree 3 is

$$Q(\delta) = 3719 + 6224\delta + 6815\delta^2 + \delta^3.$$

To reduce the polynomials, we also use

$$\begin{aligned} Q_2(\delta_2) &= 6224 + 6815\delta_1 + \delta_1^2 + 6815\delta_2 + \delta_1\delta_2 + \delta_2^2, \\ Q_3(\delta_3) &= 6815 + \delta_1 + \delta_2 + \delta_3. \end{aligned}$$

The coefficient vector for u_2 can be determined.

$$u_2 = \begin{pmatrix} 3545 + 5594\delta_1 + 7211\delta_1^2 \\ 2430 + 3223\delta_1 + 5243\delta_1^2 \\ 5815 + 2763\delta_1 + 4423\delta_1^2 \\ 1580 + 7062\delta_1 + 6221\delta_1^2 \\ 3024 + 5271\delta_1 + 1491\delta_1^2 \end{pmatrix}^T \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix}.$$

Next, we find $\delta_1 = 5205$.

The remaining polynomial of degree 2 with solutions δ_2 and δ_3 is

$$R(\delta) = 5473 + 4167\delta + \delta^2.$$

The diversity of the zeros leads to the polynomial

$$R_2(\delta) = 4167 + \delta_2 + \delta_3.$$

u_3 is expressed by

$$u_3 = \begin{pmatrix} 2432 + 5267\delta_2 \\ 4465 + 4422\delta_2 \\ 4285 + 3138\delta_2 \\ 411 + 1450\delta_2 \\ 4048 + 2253\delta_2 \end{pmatrix}^T \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{pmatrix}.$$

It follows $\delta_2 = 1595$, $\delta_3 = 2091$ and

$$\begin{aligned} u_4 &= (2959, 213, 828, 7616, 4183) \cdot (y_1, \ldots, y_5)^T, \\ u_1 &= (3915, 6581, 103, 5283, 6168) \cdot (y_1, \ldots, y_5)^T, \\ u_5' &= (623, 1900, 1900, 747, 659) \cdot (y_1, \ldots, y_5)^T. \end{aligned}$$

The variable transformation A':

$$A' = \begin{pmatrix} 3915 & 6581 & 103 & 5283 & 6168 \\ 4890 & 5665 & 3204 & 2934 & 3043 \\ 587 & 5561 & 7034 & 4379 & 909 \\ 2959 & 213 & 828 & 7616 & 4183 \\ 623 & 1900 & 1900 & 747 & 659 \end{pmatrix}.$$

The representation matrix of the missing fifth equation:

$$C_5' = \begin{pmatrix} 412 & 4790 & 6093 & 3711 & 2245 \\ 4790 & 3156 & 3975 & 7208 & 2991 \\ 6093 & 3975 & 1594 & 7813 & 7386 \\ 3711 & 7208 & 7813 & 1858 & 152 \\ 2245 & 2991 & 7386 & 152 & 513 \end{pmatrix}.$$

The matrix of the linear combinations:

$$B' = \begin{pmatrix} 1002 & 2720 & 5454 & 4063 & 1482 \\ 4493 & 3035 & 2520 & 3937 & 408 \\ 6472 & 190 & 6315 & 445 & 6145 \\ 5106 & 4728 & 3318 & 777 & 552 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The matrices A' and B' form the secret key.

□ □ □