Using the Trace Operator to repair the Polynomial Reconstruction based Cryptosystem presented at Eurocrypt 2003

D. Augot, M. Finiasz and P. Loidreau

ENSTA, INRIA
Daniel.Augot@inria.fr, Matthieu.Finiasz@inria.fr, loidreau@ensta.fr

Abstract. In this paper, we present a modification of the Augot-Finiasz cryptosystem presented at EUROCRYPT 2003. Coron managed to design an attack against the original cryptosystem enabling an attacker to decrypt any intercepted ciphertext efficiently. We introduce here a modification of the scheme which appears to resist to this attack. We furthermore propose parameters thwarting the state of the art attacks.

1 Introduction

At the Eurocrypt 2003 Conference, Augot and Finiasz [1] presented a new public-Key cryptosystem supposedly based upon the problem of polynomial reconstruction (hereafter denoted PR problem) : given n, k, t and $(g_i, y_i)_{i=1...n}$ n couples in $GF(q^u)$, find any polynomial $p[X]$ of degree less than k such that $p(g_i) = y_i$ for at least t values of i.

As analysed in [8], this problem seems to be hard, and therefore would provide a solid ground to design public key cryptosystems. Basically, the original scheme in [1] uses as a public-key a word of a Reed-Solomon code scrambled by the addition of an error-vector of sufficiently large Hamming weight such that the PR problem is intractable. Note that the conditions under which the problem is tractable are given by Guruswami and Sudan in [6]. Additionally to being an alternative to the existing public key encryption scheme based on the factorization or on discrete logarithm problems, the system provided a solution to the reminiscent large key-size problem of some encryption scheme such as McEliece system or HFE. Namely, the authors proposed in particular a system with a key of 3072 bits for a security of 2^{80} binary operations.

This system however was broken by Coron in polynomial-time, exploiting a linear transformation used in the encryption step [3]. He designed a variant of the Welch-Berlekamp decoding algorithm for Reed-Solomon codes [10] which constructs a univariate polynomial of low degree whose roots contains one security parameter. Since the number of its roots is upper-bounded by the low degree of the polynomial, this polynomial is easily factored and the system can be broken in polynomial-time. A further analysis of the system and of Coron's attack was given by Kiayias and Yung in [7]. They also proposed a modification to resist Coron's attack, but this modification is still insecure.

All these attacks are cyphertext-only, and recover the plaintext corresponding to any ciphertext, without breaking the given instance of the PR problem. This demonstrate that the encryption function is not one-way, and that there is no reduction of an attack of the system to an algorithm solving the PR problem (thus no security proof).

Here, we show that a simple modification of the scheme, using properties of the well-known Trace operator over finite fields, can thwart Coron's attack.

In the first Section, we recall how Reed-Solomon codes are constructed and we define the Trace operator. Then, in Section 2, we recall the original system and present quickly the principle of Coron's attack. Finally, we present in Section 3 the system that is almost the same as the original one except that the structure is scrambled by using properties of the Trace operator. We show that this system resists all known attacks including Coron's attack. We conclude with a proposal of a resistant set of parameters for the new system.

2 Reed-Solomon Codes and Trace Operator

In this section we present algebraic tools used later in the paper for the design of the system and for its security analysis. Reed-Solomon codes are well-known optimal codes and are closely related to the rings of univariate polynomials over finite fields.

Consider a finite field $\mathrm{GF}(q^u)$, where q is the power of a prime number. With these notations, the finite field $\mathrm{GF}(q)$ is a subfield of $\mathrm{GF}(q^u)$. Let us consider a list

$$S = (g_1, g_2, \ldots, g_n)$$

of n distinct elements in $\mathrm{GF}(q^u)$, denoted hereafter *the support*. Let ev_S denote the evaluation of polynomials on the elements of S, *i.e.*

$$\mathrm{ev}_S \begin{cases} \mathrm{GF}(q^u)[X] \longrightarrow \mathrm{GF}(q^u)^n \\ p(X) \qquad\quad \longmapsto (p(g_1), p(g_2), \ldots, p(g_n)), \end{cases}$$

where $\mathrm{GF}(q^u)[X]$ is the set of univariate polynomials with coefficients in $\mathrm{GF}(q^u)$.

Definition 1 *The Reed-Solomon code of dimension k and of support S is*

$$RS_k(S) = \{\mathrm{ev}_S(f) \mid f \in GF(q^u)[X] \text{ and } \deg(f) < k\}.$$

The code $RS_k(S)$ can correct up to $\lfloor (n-k)/2 \rfloor$ corrupted positions in polynomial time by using a Berlekamp-Massey or Welsh-Berlekamp algorithm [10].

The finite field $\mathrm{GF}(q^u)$ can be viewed as a u-dimensional vector space over $\mathrm{GF}(q)$. Let $\gamma_1, \ldots, \gamma_u$ be a basis of $\mathrm{GF}(q^u)$ over $\mathrm{GF}(q)$, then every element $\alpha \in \mathrm{GF}(q^u)$ can be uniquely written $\alpha = \sum_{i=1}^{u} a_i \gamma_i$, where $a_i \in \mathrm{GF}(q)$.

Definition 2 *The Trace operator of GF(q^u) into GF(q) is defined by*

$$\forall x \in GF(q^u),\ \ Tr(x) = x + x^q + \cdots + x^{q^{u-1}}$$

The Trace operator is a GF(q)-linear (and not GF(q^u)) mapping of GF(q^u) into GF(q). It defines a scalar product over GF(q^u). For any basis $\gamma_1, \ldots, \gamma_u$ of GF(q^u), there exists a unique dual basis $\gamma_1^\star, \ldots, \gamma_u^\star$ with respect to the scalar product induced by the Trace operator. That is, we have

$$\mathrm{Tr}(\gamma_i \gamma_i) = 1 \text{ and } \mathrm{Tr}(\gamma_i \gamma_j) = 0, \text{ if } i \neq j.$$

We note also that this dual basis can be easily computed. We also extend the action of the Trace operator to vectors $c = (c_1, \ldots, c_n)$ as $\mathrm{Tr}(c) = (\mathrm{Tr}(c_1), \ldots, \mathrm{Tr}(c_n))$. The fundamental proposition linking the Trace operator and some Reed-Solomon codes is the following:

Proposition 1 *Let $S = (g_1, \ldots, g_n)$ where $g_i \in GF(q)$ for all $i = 1, \ldots, n$ (i.e. the g_i's all belong to the* subfield *of GF(q^u)) . Then for all $c = ev_S(p)$ with $p(X) = \sum_{i=0}^{k-1} p_i X^i \in GF(q^u)[X]$ (polynomials with coefficients in the* extension *field), we have*

$$Tr(c) = ev_S(P),$$

where $P(X) = \sum_{i=0}^{k-1} Tr(p_i) X^i$.

Furthermore the corresponding Reed-Solomon code $RS_k(S)$ is stable under the action of the Trace operator.

Proof. Since $c = ev_S(p)$, for every component c_j of c, we have $c_j = p(g_j) = \sum_{i=0}^{k-1} p_j g_i^j$. Since $g_j \in \mathrm{GF}(q)$ and by GF(q)-linearity of the trace operator, for all j we have $\mathrm{Tr}(c_j) = \sum_{i=0}^{k-1} \mathrm{Tr}(p_i) g_j^i = \mathrm{ev}_S(P)_j$.

3 Original system

First, we describe the original system as presented in [1], then, we describe Coron's attack.

3.1 Description

The original system is the following:

- *Known Parameters:* GF(q^u), integers $n,\ k,\ W,\ w$, a set $S = (g_1, \ldots, g_n)$ of n distinct elements over GF(q^u).
- *Key generation:* Alice chooses randomly a monic polynomial $p(X)$ of degree $k-1$ over GF(q^u), and computes $c = \mathrm{ev}_S(p)$. The vector c belongs thus to $RS_k(S)$. Then she generates randomly a vector $E = (E_1, \ldots, E_n) \in \mathrm{GF}(q^u)^n$ with exactly W non-zero coordinates. The public-key consists of $K = c + E$. Both c and E remain secret.

– *Encryption:* Bob wants to send a message $m_0 = (m_{0,0}, \ldots, m_{0,k-2})$ of length $k-1$ over $\mathrm{GF}(q^u)$ to Alice. First he transforms m_0 into the polynomial $m_0(X) = \sum_{i=0}^{k-2} m_{0,i} X^i$ and computes $m = \mathrm{ev}_S(m_0)$. Then he picks up randomly $\alpha \in \mathrm{GF}(q^u)$, and a vector e of length n with w non-zero coordinates. The ciphertext that Bob sends to Alice is

$$y = m + \alpha K + e.$$

– *Decryption:* Alice first shortens the ciphertext on the non-zero positions of E by removing all coordinates corresponding to the non-zero positions of E. She obtains $\overline{y} = \overline{m} + \alpha\overline{c} + \overline{e}$, where the overlining operation denotes shortening the vectors. Hence we obtain $\overline{K} = \overline{c}$. Since a shortened Reed-Solomon code is still a Reed-Solomon code, with a different support, it is still decodable. Therefore by one decoding step in the shortened Reed-Solomon code, Alice recovers $\overline{m} + \alpha\overline{c}$. Since $\overline{m} = \mathrm{ev}_{\overline{S}}(m_0)$ and $\alpha\overline{c} = \mathrm{ev}_{\overline{S}}(\alpha p)$ and since the degree of m_0 is less than the degree of p, Alice first recovers $Q(X) = m_0(X) + \alpha p(X)$ by interpolation. Then, by considering that the highest coefficient of Q is α, she recovers α, and finally m_0.

The security analysis of the system given in [1] shows that the system, with carefully selected parameters, can resist all previously known decoding attacks, like error set decoding and information set decoding with a public key relatively small (a few thousand bits). The authors proposed the following parameters: $\mathrm{GF}(q^u) = \mathrm{GF}(2^{84})$, $n = 1024$, $W = 74$, ensuring that the PR problem is intractable and $w = 25$, ensuring a security of at least 2^{80} against decoding attacks. Now, with such parameters, the size of the public key $c + E$ is equal to $84 \times 1024 = 84$ kbits.

3.2 Coron's Attack

Coron designed a very efficient ciphertext only attack able to recover the scrambling element $\alpha \in \mathrm{GF}(q^u)$ in polynomial time, see [3]. When α is known, one can easily recover the plaintext as stated in [1]. To achieve this, he modifies the Welsh-Berlekamp algorithm, and builds a polynomial of low degree vanishing at the element α.

Suppose Eve intercepts a ciphertext y. To recover the plaintext m_0, she has to solve the equation $y = \mathrm{ev}_S(m_0) + \alpha K + e$. Then, Eve has to solve the following system in the unknowns $m_0(X), \alpha$, and e_i.

$$y_i = m_0(g_i) + \alpha K_i + e_i, \quad i = 1, \ldots, n,$$

where m_0 is a polynomial of degree less than $k-1$, the e_i's are equal to 0 except on w positions, and $\alpha \in \mathrm{GF}(q^u)$. Solving this system is equivalent to solving the system in the unknowns $Z(X)$, α, and $m_0(X)$

$$\forall i = 1, \ldots, n, \;\; Z(g_i)(y_i - \alpha K_i) = m_0(g_i) Z(g_i), \tag{1}$$

where $Z(X)$ is a non-zero polynomial over GF(q^u) of degree at most w. If this system is expanded it leads to a quadratic system. Following the principle of the Berlekamp-Welsh algorithm, Coron linearizes the system by introducing the following system in the new unknowns $Z(X)$, α, and $N(X)$:

$$\forall i = 1, \ldots, n,\ Z(g_i)(y_i - \alpha K_i) = N(g_i), \tag{2}$$

where $N(X)$ is now a non-zero polynomial over GF(q^u) of degree at most $k + w - 2$. A solution to system (1) also gives a solution to system (2). Thus, by getting every solution of system (2) one gets necessarily a solution for decrypting the intercepted ciphertext. These equations still form a quadratic system in the coefficients of $Z(X)$, α and the coefficients of $N(X)$. However, let us consider the matrix of the system

$$M(x) = \begin{pmatrix} y_1 - xK_1, \cdots (y_1 - xK_1)g_1^w, 1, g_1, \cdots g_1^{k+w-2} \\ y_2 - xK_2, \cdots (y_2 - xK_2)g_2^w, 1, g_2, \cdots g_2^{k+w-2} \\ \vdots \quad \ddots \quad \vdots \quad \vdots \ddots \vdots \\ y_n - xK_n, \cdots (y_n - xK_n)g_n^w, 1, g_n, \cdots g_n^{k+w-2} \end{pmatrix}.$$

This matrix has the known parameters y_i's, K_i's and g_i's and x as an indeterminate. The condition to have a solution $Z(X)$, α, $B(X)$ to the system 2 is that $M(\alpha)$ is not of maximal rank. Hence α is a root of the determinant of any square submatrix of $M(x)$. Any such determinant is a univariate polynomial over GF(q^u) of degree at most $w + 1$. By computing a few determinants and computing their greatest common divisors, Eve finds α very easily (recall that w is small) recovering thus the plaintext in polynomial time. Eve can also compute the roots of a particular determinant and try the different roots into the system to check which one is the right one. With the originally proposed parameters $n = 1024,\ k = 900, w = 25, W = 74$, and $q = 2^{80}$, Coron demonstrate that it takes about 30 minutes of computation on a standard PC to recover the plaintext from the ciphertext [3].

For completeness, Coron proposed a case 2 version which must be used in particular cases. This happens whenever $M(0)$ is not of full rank. By choosing well the submatrices Eve could even recover the elements of the secret key. Kiayias and Yung showed that this configuration is very rare [7].

4 The New System

With some simple algebraic considerations, we can thwart this attack without increasing the size of the public key. This modification produces a system that is somehow better than the original one. Indeed, it increases the speed of the system and decreases the block size.

The idea itself was contained in the original paper. It consisted in taking the public key with respect to a subfield subcode of the Reed-Solomon code. Considering subcodes of very structured codes is usually a good idea for scrambling

their structure. The best example of it is without contest the McEliece system. Whereas it was shown that using the family of Generalized Reed-Solomon codes was extremely weak, using the family of Goppa codes – which are subfield subcodes of Generalized Reed-Solomon codes – is secure against all types of structural attacks. Behind these considerations we find once again the Trace operator that is intimately linked with the notion of subfield subcode, see [4]. This led us to design a system based on the model of Augot and Finiasz's using an additional scrambling by means of this very Trace operator. Let it be described as follows.

- *Known Parameters of the system:* a finite field $\mathrm{GF}(q^u)$, integers n, k, W, w. a set of $S = (g_1, \ldots, g_n)$ of n distinct elements of $\mathrm{GF}(q) \subset \mathrm{GF}(q^u)$.
- *Key generation:* Alice secretly generates a polynomial $p(X) = \sum_{i=0}^{k-1} p_i X^i$ over $\mathrm{GF}(q^u)$, with the following properties: the u coefficients $p_{k-1}, \ldots, p_{k-u}$ are such that they form a basis of $\mathrm{GF}(q^u)$ over $\mathrm{GF}(q)$. She computes $c = \mathrm{ev}_S(p)$. The vector c belongs thus to $RS_k(S)$. Then she generates a vector $E = (E_1, \ldots, E_n) \in \mathrm{GF}(q^u)^n$ with exactly W non-zero coordinates. The public-key is the vector $K = c + E$ over $\mathrm{GF}(q^u)$. Both c and E remain secret.
- *Encryption:* Bob wants to send a message $m_0 = (m_{0,0}, \ldots, m_{0,k-u-1})$ of length $k-u$ over $\mathrm{GF}(q)$ to Alice. First he transforms m_0 into the polynomial $m_0(X) = \sum_{i=0}^{k-u-1} m_{0,i} X^i$ and computes $m = \mathrm{ev}_S(m_0)$. Then he randomly chooses an element $\alpha \in \mathrm{GF}(q^u)$ and a vector e over $\mathrm{GF}(q)$ of length n with w non-zero coordinates. The ciphertext Bob sends to Alice is

  $$y = m + \mathrm{Tr}(\alpha K) + e,$$

  where Tr denotes the trace operator of $\mathrm{GF}(q^u)$ onto $\mathrm{GF}(q)$ (see Definition 2).
- *Decryption:* this step is almost identical to the decryption step of the original scheme. Alice first shortens the ciphertext on the non-zero positions of E. She obtains $\overline{y} = \overline{m} + \mathrm{Tr}(\alpha\overline{c}) + \overline{e}$, where the overlining operation denotes shortening the vectors. Remember that S was chosen to de defined over $\mathrm{GF}(q)$, thus, by Proposition 1 $\mathrm{Tr}(\alpha\overline{c}) \in RS_k(\overline{S})$, the Reed-Solomon code of support $\overline{S}$, of length $n-W$ and dimension k, which has a decoding algorithm. By one decoding step in $RS_k(\overline{S})$, Alice recovers $\overline{m} + \mathrm{Tr}(\alpha\overline{c})$. We have $\overline{m} = \mathrm{ev}_{\overline{S}}(m_0)$, and $\mathrm{Tr}(\alpha\overline{c}) = ev_{\overline{S}}(P)$ where $P(X) = \sum_{i=0}^{k-1} \mathrm{Tr}(\alpha p_i) X^i$. Thus, by polynomial interpolation, she recovers the unique polynomial $Q(X) = \sum_{i=0}^{k-1} q_i X^i$ of degree $k-1$ over $\mathrm{GF}(q)$ such that $\mathrm{ev}_{\overline{S}}(Q) = \overline{m} + \mathrm{Tr}(\alpha\overline{c})$, that is $Q(X) = m_0(X) + P(X)$. Since m_0 has degree less than $k-u-1$, we have

  $$q_i = \mathrm{Tr}(\alpha p_i), \quad \text{for } i = k-u, \ldots, k-1,$$

  by identification of high degree terms.
  By the property of the Trace operator, the $\mathrm{Tr}(\alpha p_i)$ for $i = k-u, \ldots, k-1$ are exactly the u coordinates of α in the dual basis of $p_{k-1}, \ldots, p_{k-u}$. This gives

us directly α with no additional cost. Knowing α one gets the polynomial P whose coefficients are the $\mathrm{Tr}(\alpha p_i)$ for $i = 0, \ldots, k-1$. Finally Alice gets the plaintext $m_0(X) = Q(X) - P(X)$.

In order to generate the public-key, Alice has to pick up a basis of $\mathrm{GF}(q^u)$ over $\mathrm{GF}(q)$. Since the number of such bases is very high, picking up randomly u elements in $\mathrm{GF}(q^u)$ and testing if they form a basis is a good way to proceed.

Considering that an arithmetic operation over $\mathrm{GF}(q^u)$ costs $O(u^2 log^2 q)$ binary operations, the total cost of the algorithm is:

- *Encryption*: the Trace can be computed $\mathrm{O}(u)$ time. Thus the encryption costs $\mathrm{O}(nu\log q)$ binary operations per bit of plaintext.
- *Decryption*: the operations take place in $\mathrm{GF}(q)$, and not in $\mathrm{GF}(q^u)$. The cost of decoding in the shortened Reed-Solomon code is thus equal to $\mathrm{O}((n - W)^2 \log^2 q)$. The polynomial Q can be interpolated in $\mathrm{O}((n - W)^2 \log^2 q)$ operations. To find the plaintext m_0, one computes the difference of two polynomials of over $\mathrm{GF}(q^u)$, that is $k - u - 1$ additions over $\mathrm{GF}(q^u)$. This can be neglected. Finally, since u is small, the cost of decryption is roughly $\mathrm{O}((n - W)^2 \log\, q/k)$ binary operations per bit of plaintext.

Note that in the following, we deal with a field $\mathrm{GF}(q)$ small enough to be implemented in software or even in hardware. That is, we can consider that the operations in $\mathrm{GF}(q)$ have a constant cost. This improves considerably the efficiency of the system.

5 Security of the New System

The security of the system against the previously known decoding attacks was investigated at length in Augot and Finiasz's paper, and we can reuse the results here. To ensure a sufficient security, one has to choose good parameters. We show how Coron's approach can be modified into either finding the roots of a polynomial of exponential degree or solving an overdefined multivariate system, but with very large equations. In the last Section, we propose parameters for the system to be secure.

5.1 Coron-like attacks

We study how Coron's approach must be modified to be applied to the modified system. Originally it consisted in finding the roots of a polynomial of degree $w + 1$ over a large finite field. In the new system, we have

$$y = \mathrm{ev}_S(m_0) + \mathrm{Tr}(\alpha K) + e, \tag{3}$$

where m_0 is a polynomial of degree $k - u - 1$, the e_i's are equal to 0 except for w positions, and $\alpha \in \mathrm{GF}(q^u)$. Solving this system is equivalent to solving the system in the unknowns $Z(X)$, α, and $m_0(X)$

$$\forall i = 1, \ldots, n, \quad Z(g_i)(y_i - \mathrm{Tr}(\alpha K_i)) = m_0(g_i)Z(g_i), \tag{4}$$

where $Z(X)$ is a non-zero polynomial over $\mathrm{GF}(q)$ of degree at most w.

There are two different approaches to deal with: the univariate approach and the multivariate approach. Both derive from the properties of the Trace operator.

Univariate approach

A solution to system (4) is a solution to the following system in the unknowns $Z(X)$, α, and $N(X)$,

$$\forall i = 1 \ldots n, \; Z(g_i)(y_i - \mathrm{Tr}(\alpha K_i)) = N(g_i), \tag{5}$$

where $N(X)$ is a non-zero polynomial over $\mathrm{GF}(q)$ of degree at most $k + w - u - 1$. Let

$$M_{\mathrm{Tr}}(x) = \begin{pmatrix} y_1 - \mathrm{Tr}(xK_1), \cdots (y_1 - \mathrm{Tr}(xK_1))g_1^w, \, 1, \, g_1, \cdots g_1^{k+w-u-1} \\ y_2 - \mathrm{Tr}(xK_2), \cdots (y_2 - \mathrm{Tr}(xK_2))g_2^w, \, 1, \, g_2, \cdots g_2^{k+w-u-1} \\ \vdots \qquad\qquad \ddots \qquad\qquad \vdots \qquad\qquad \vdots \; \ddots \; \vdots \\ y_n - \mathrm{Tr}(xK_n), \cdots (y_n - \mathrm{Tr}(xK_n))g_n^w, \, 1, \, g_n, \cdots g_n^{k+w-u-1} \end{pmatrix},$$

where $\mathrm{Tr}(x) = \sum_{i=0}^{q^{u-1}} x^{q^i}$ is a polynomial over $\mathrm{GF}(q)$ of degree q^{u-1}. The element α is such that $M_{\mathrm{Tr}}(\alpha)$ is not of maximal rank. Thus α is a root of the determinant of any square submatrix of $M_{Tr}(x)$.

Now the constatation is made that the determinants are polynomials over $\mathrm{GF}(q)$ of degree $(w+1)q^{u-1}$. Therefore, since computing the roots or the greatest common divisors of polynomials is polynomial in complexity with the degree, it becomes rapidly intractable to find the common root or to factor of these polynomials.

The second case in Coron's attack cannot happen here. Indeed, the polynomials have a too large degree to be uniquely interpolated from the n components of the support S.

Multivariate approach

Let $\gamma_1, \ldots, \gamma_u$ be a basis of $\mathrm{GF}(q^u)$ over $\mathrm{GF}(q)$. Let

$$\alpha = \sum_{t=1}^{u} a_t \gamma_t,$$

and let $K_{i,j} = \mathrm{Tr}(\gamma_i K_j)$. Finding a solution to system (4) is now equivalent to solve the following system in the unknowns $Z(X)$, $a_1, \ldots, a_u$, and $m_0(X)$.

$$\forall i = 1, \ldots, n \quad Z(g_i)\left(y_i - \sum_{t=1}^{u} a_t K_{t,i}\right) = Z(g_i)m_0(g_i). \tag{6}$$

We consider the following system in the unknowns $Z(X)$, $a_1, \ldots, a_u$, and $N(X)$.

$$\forall i = 1, \ldots, n \quad Z(g_i) \left(y_i - \sum_{t=1}^{u} a_t K_{t,i} \right) = N(g_i). \tag{7}$$

where Z has degree at most w, and N is a non-zero polynomial over GF(q) of degree at most $k + w - u - 1$.

A solution to system (6) is also a solution to system (7): if $Z, a_1, \ldots, a_u$, and m_0 are solutions to system (6) then $Z,\ a_1, \ldots,\ a_u$, and $N = Z \cdot m_0$ are solutions to system (7). By following step by step Coron's approach we first expand the polynomials.

Let $Z(X) = \sum_{i=0}^{w} z_i X^i$ and let $N(X) = \sum_{i=0}^{k+w-u-1} t_i X^i$. Let us define

$$M(x_1, \ldots, x_u) = \begin{pmatrix} y_1 - \sum_{t=1}^{u} x_t K_{t,1}, & \cdots & (y_1 - \sum_{t=1}^{u} x_t K_{t,2}) g_1^w, & 1, & g_1, & \cdots & g_1^{k+w-u-1}, \\ y_2 - \sum_{t=1}^{u} x_t K_{t,2}, & \cdots & (y_2 - \sum_{t=1}^{u} x_t K_{t,2}) g_2^w, & 1, & g_2, & \cdots & g_2^{k+w-u-1}, \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \\ y_n - \sum_{t=1}^{u} x_t K_{t,n}, & \cdots & (y_n - \sum_{t=1}^{u} x_t K_{t,n}) g_n^w, & 1, & g_n, & \cdots & g_n^{k+w-u-1}, \end{pmatrix},$$

and $Y = (z_0, \ldots, z_w, t_0, \ldots, t_{k+w-u-1})$. Solving system (7) is equivalent to solve the following equation in the unknowns $Y, a_1, \ldots, a_u$.

$$M(a_1, \ldots, a_u) \cdot Y^t = 0, \tag{8}$$

The known existence of a non-trivial solution to this equation implies that $M(a_1, \ldots, a_u)$ is not of maximal rank. For any square submatrix $M'(x_1, \ldots, x_u)$, we must have $Det(M'(a_1, \ldots, a_u)) = 0$. Every such determinant of the form $Det(M'(x_1, \ldots, x_u))$ is a multivariate polynomial of degree $w+1$ in u unknowns.

To get a solution, one has to compute the Groebner basis of the system, since the number of solutions will be relatively small. However computing the Groebner basis is a very difficult problem, and at least the complexity is hard to evaluate.

6 Proposition of parameters

The authors wish to thank here Jean-Sébastien Coron, for fruitful discussion. He pointed out a new attack on the modification of the system which enables to recover the private-key from the public-one if one is not careful enough. In the building of our parameters, we took into account his remarks.

We consider the following parameters:

- The chosen fields are GF(q^u) = GF(2^{80}), GF(q) = GF(2^{20}) (thus $u = 4$)
- We take $n = 2048$, the size of the public-key is thus equal to 160 kbits, that is twice as large as for the original parameters.
- Then $W = 546$ is sufficient to resist all attacks against the public-key. We took into account Coron's remarks.
- Finally $w = 49$.

Compared to the original system, the block size is smaller. Namely a plaintext consists of $k-u$ elements in $\mathrm{GF}(2^{20})$, that is 27920 bits. The transmission rate is $\approx 68\%$. These parameters are resistant to the previously known decoding attack given in [1].

Another advantage compared to the original system is that the computations are done in a small field that is to know $\mathrm{GF}(2^{20})$. This field can be implemented in software or hardware very easily, decreasing thus the complexity of the scheme.

Now we can study the resistance of the scheme against different approaches.

Univariate approach

As stated in the previous section, Eve has to compute the roots of a polynomial of degree $49 \times 2^{60} \approx 2^{65}$ over $\mathrm{GF}(2^{80})$, or greatest common divisors of at least two of these polynomials, which is intractable, and costs more that 2^{80} even if the polynomials are sparse ones.

Multivariate approach

In that case Eve has to find the Groebner basis over $\mathrm{GF}(2^{20})$ of a set of equations of degree 49 in 4 unknowns. Experimentally by taking smaller parameters, each equation has many terms, which gives a system of equations each having approximately 2^{20} non zero terms. This should be a difficult system to solve, but no complexity estimation can be derived yet.

7 Conclusion

In this paper we have proposed a new version of the Augot-Finiasz cryptosystem based on the polynomial reconstruction problem. It is as simple of use and of design as the original one and is now secure against Coron's attack, which breaks in polynomial time the original cryptosystem.

We proposed parameters for the system to be secure against state of the art attacks. While the size of the public-key has to be increased, the system also gains in efficiency, with a smaller block size.

References

1. D. Augot and M. Finiasz. A public key encryption scheme bases on the polynomial reconstruction problem. In *EUROCRYPT 2003*, pages 222–233, 2003.
2. Anne Canteaut and Florent Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense bch codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.
3. J.-S. Coron. Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem. Cryptology ePrint Archive, Report 2003/036, 2003. http://eprint.iacr.org/.
4. P. Delsarte. On subfield subcodes of modified Reed–Solomon codes. *IEEE Transactions on Information Theory*, 20:575–576, 1975.

5. E. M. Gabidulin. Public-key cryptosystems based on linear codes over large alphabets: efficiency and weakness. In P. G. Farrell, editor, *Codes and Cyphers*, pages 17–31. Formara Limited, Southend-on-sea, Essex, 1995.
6. V. Guruswami and M. Sudan. Improved decoding of Reed–Solomon and algebraic geometric codes. *IEEE Transactions on Information Theory*, 45:1757–1767, 1999.
7. A. Kiayias and M. Yung. Cryptanalysis of the the polynomial reconstruction based public-key cryptosystem of eurocrypt'03 in the optimal parameter setting. Available on http://www.cse.uconn.edu/~akiayias/, 2003.
8. A. Kiayias and M. Yung. Cryptographic hardness based on the decoding of Reed–Solomon codes. In *Proceedings of ICALP 2002*, volume 2380 of *LNCS*, pages 232–243, 2003.
9. V. S. Pless and W. C. Huffman, editors. *Handbook of Coding Theory*. Elsevier Science B.V., 1998.
10. L. R. Welsh and E. R. Berlekamp. Error correction for algebraic block codes, 1986. US Patent 4 633 470.