Cryptanalyzing the Polynomial-Reconstruction based Public-Key System Under Optimal Parameter Choice

Aggelos Kiayias[1] and Moti Yung[2]

[1] Department of Computer Science and Engineering,
University of Connecticut, Storrs, CT, USA
aggelos@cse.uconn.edu
[2] Department of Computer Science,
Columbia University, New York, NY, USA
moti@cs.columbia.edu

Abstract. Recently, Augot and Finiasz presented a coding theoretic public key cryptosystem that suggests a new approach for designing such systems based on the Polynomial Reconstruction Problem. Their cryptosystem is an instantiation of this approach under a specific choice of parameters which, given the state of the art of coding theory, we show in this work to be sub-optimal. Coron showed how to attack the Augot and Finiasz cryptosystem. A question left open is whether the general approach suggested by the cryptosystem works or not. In this work, we show that the general approach (rather than only the instantiation) is broken as well. Our attack employs the recent powerful list-decoding mechanisms.

1 Introduction.

Recently, in Eurocrypt 2003 [AF03], Augot and Finiasz presented a public-key cryptosystem that was based on the Polynomial Reconstruction problem (PR). This scheme suggests a general approach for designing such cryptosystems; their cryptosystem is an instantiation of this approach based on a specific choice of parameters.

Let us first review PR, which is a curve-fitting problem that has been studied extensively especially in the coding theoretic setting, where it corresponds to the Decoding Problem of Reed-Solomon Codes.

Definition 1. Polynomial Reconstruction *(PR) Given a set of points over a finite field* $\{\langle z_i, y_i\rangle\}_{i=1}^{n}$*, and parameters* $[n, k, w]$*, recover all polynomials* p *of degree less than* k *such that* $p(z_i) \neq y_i$ *for at most* w *distinct indexes* $i \in \{1, \ldots, n\}$*.*

Regarding the solvability of PR, we remark that unique solution can only be guaranteed when $w \leq \frac{n-k}{2}$ (the error-correction bound of Reed-Solomon Codes). For such parameter choices, the Berlekamp-Welch Algorithm [BW86] can be used to recover the solution in polynomial-time. When the number of errors w exceeds this bound, unique solution is not necessarily guaranteed. In this range, a decoding algorithm may output a list of polynomials that satisfy the constraints. This is called list-decoding and recently some breakthrough results have been achieved in this field. The most powerful list-decoding algorithm is the one by Guruswami and Sudan, [GS98]. The algorithm will work for any number of errors such that $w < n - \sqrt{(k-1)n}$. For choice of parameters beyond the Guruswami-Sudan solvability bound, no known efficient algorithm exists that solves PR (and [GS98] gives some indication why such an algorithm is not likely to be found).

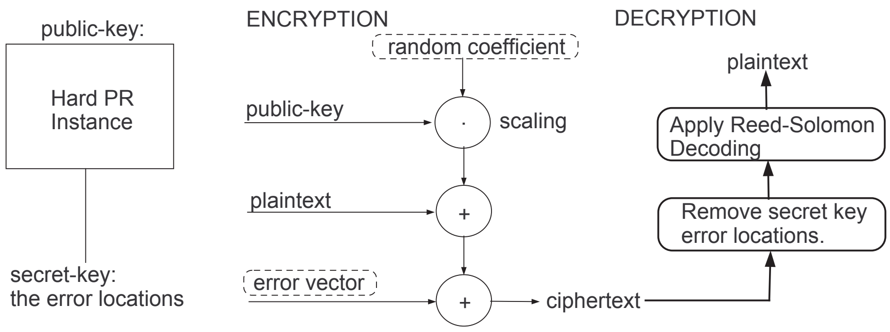

Fig. 1. The Augot and Finiasz general approach for designing a pk-cryptosystem using the hardness of RS decoding.

Augot and Finiasz's general approach (see figure 1) is to use a PR instance which is hard to solve (i.e., a highly noisy instance) as a public key, and to encrypt a message by scaling the given public key (i.e., multiplying the polynomial values by a scalar) and adding to the scaled instance the message which is represented as a slightly lower degree second PR instance which is solvable, yielding a PR instance representing the ciphertext. The receiver who knows the noise locations in the public key can recover the message. The approach allows key sizes that are much smaller than the traditional coding theoretic based public-key systems (i.e., the McEliece cryptosystem [McE78]). Further, direct use of the above mentioned decoding and list-decoding methods do not apply to breaking the cryptosystem (directly). To implement the approach of figure 1 one needs to specify: (i) the structure of the public-key, (ii) the structure of the error-vector, and in accordance (iii) the decoding method employed in decryption.

What we noticed is that while the public-key structure was chosen to be an unsolvable PR instance, the choice of the error-vector and the associated decoding method was sub-optimal considering the state-of-the-art of Coding

Theory. The scheme was in fact, based on unique decoding (and not list decoding techniques) and did not consider probabilistic analysis to maximize the allowed entropy of the error-vector.

The scheme of [AF03] was recently broken by Coron [Cor03a,Cor03c] (without affecting the solvability of PR). The elegant attack presented in [Cor03c] is in fact a ciphertext-only attack that is built on the Berlekamp-Welch method and recovers the message, given knowledge only of the public-key and a ciphertext. A further modification of the scheme, using extension fields but essentially the same system, was suggested recently [AFL03] and was shown by Coron [Cor03b] to be vulnerable to essentially the same attack.

Coding Theoretic Motivation. The Augot-Finiasz cryptosystem employed unique decoding techniques rather than list-decoding techniques (assuming that unique decoding is what is needed for a correct cryptosystem — an assumption we refute herein). Moreover, they consider only worst-case analysis in the selection of the code parameters. Thus, their cryptosystem is sub-optimal in the above respects given the general approach outlined above.

This leaves open the question of whether this general approach works in principle, i.e., when one uses the optimal coding theoretic techniques and probabilistic analysis for the parameter selection.

Our Results: In this work we investigate the above question. In particular, we maximize the rate of the error vector used during encryption and choose state-of-the-art list-decoding techniques to implement the Reed-Solomon decoding step for decryption. Regarding the optimization (maximization) of the error-rate we make two key observations (1) the system of [AF03] employs a worst-case approach in selecting this parameter; a probabilistic approach (that we perform in this work) allows higher values. (2) the system of [AF03] employs Berlekamp-Welch RS-decoding for the decryption operation. We emphasize that more powerful decoding techniques can be employed that allow larger values for the error-rate parameter. Our methodology is to use an extended set of tools both for design and analysis in order to get the best possible instantiations of the general approach. The tools include "list decoding" rather than unique decoding techniques (which we show to be still good for decryption, since decoding to a unique value is assured with extremely high probability over a large enough field, even when ambiguous decoding is allowed, cf. Lemma 1).

We develop our presentation as a ping-pong game between a cryptosystems designer and a cryptanalyst. To avoid any misunderstanding our goal is not to design a new cryptosystem, but rather using the design and cryptanalysis steps as a methodology for exploring the general approach.

First Step. Regarding our key-observation (1) we employ the tails of the hypergeometric distribution to show that the original scheme allowed too few errors in the error-vector to be used by the message encryption process. Thus the error-rate can be increased high enough to aid the designer to achieve instances of the cryptosystem where Coron's analysis does not work. But, nevertheless we provide an alternative probabilistic analysis showing that the original attack of

Coron would work almost always even in this modified (more noisy) version, thus aiding the cryptanalyst.
Second Step. Combining our key-observations (1) and (2) above, we discover the optimal setting for the sender error-parameter ("optimal" under the assumption that the Guruswami-Sudan list-decoding algorithm [GS98] represents the best possible decoding algorithm against Polynomial Reconstruction). We show that the optimal parameter setting, helps the designer and in this case Coron's attack fails. To answer our question about the limit of the approach, we then present a new attack that is based on the Sudan and Guruswami-Sudan algorithms [Sud97,GS98]. Our attack, with overwhelming probability, breaks even the optimal parameter setting. This means that the general approach, outlined in figure 1, taken by Augot and Finiasz (rather than merely their non-optimal instantiation) breaks.

We believe that our results demonstrate how design and analysis of Coding theory based cryptography, must employ probabilistic methods and state of the art decoding techniques. Furthermore, our results and the attack of Coron demonstrate that PR-based cryptosystems that lack formal proofs of security by concrete reduction arguments, even when they seem to be related to PR, are potentially susceptible to coding theoretic attacks that do not imply any weakness in the PR problem itself. Note that, the private-key cryptosystem based on PR suggested by the authors in [KY02] was shown to be semantically secure under an intractability decisional assumption that bears upon the average-case PR (for choices of the parameters beyond the Guruswami-Sudan solvability bound). This cryptosystem (as well as the other cryptographic primitives in [KY02]) are not affected by the techniques of the present paper and of Coron's [Cor03a,Cor03b,Cor03c] and breaking these designs seems to require significant advances in RS decodability.

Due to space constraints proofs are omitted from the present abstract; the full-version with all details is available in [KY04].

2 Background: the Recent Polynomial-Based Public-Key Cryptosystem

We review the recent developments, while setting up the necessary notations and interesting points regarding our investigation.

2.1 The Cryptosystem of [AF03]

The cryptosystem of [AF03] can be described in high level as follows:

1. The public-key is a PR-instance of parameters $[n, k+1, W]$ for which (i) the hidden polynomial p is monic; (ii) solving the instance is considered hard. The public-key is a sequence of values in $(\mathbb{F} \times \mathbb{F})^n$ (while the locations of the error points is the secret key).

2. Encryption operates by first transposing (i.e., scaling the polynomial of) the public-key using a random value $\alpha \in \mathbb{F}$ (the encryption coefficient), and then adding to the transposed public-key the message (evaluated as a second polynomial represented as pairs of points using the same first coordinates as the points of the public key PR instance, with no errors), and finally adding some additional w errors. (In other words, the message is embedded in a second PR instance with w errors and added to the transposed public key). It follows that a ciphertext is a sequence of values in $(\mathbb{F} \times \mathbb{F})^n$.
3. Decryption removes the points that correspond to public-key errors, i.e., W points of the ciphertext. Decryption relies on the following two facts: (i) the remaining $n - W$ points can be decoded into a polynomial p^*; (ii) due to the fact that the message polynomial is selected to be of degree less than the degree of the monic polynomial p hidden in the public-key, it follows that the recovery of p^* implies the recovery of the encryption coefficient α. The message polynomial can be recovered as $p_{msg}(x) = p^*(x) - \alpha p(x)$.

We note that the points over which the polynomials are evaluated in a PR instance can be publicly known (thus the public-key and the ciphertext can be considered to be of size only $|\mathbb{F}|^n$).

In more detail, let $z_1, \ldots, z_n \in \mathbb{F}$ be arbitrary distinct elements of the underlying field, where $n \in \mathbb{N}$ is a security parameter. The public-key of the system is a PR-instance that is generated as follows: first a random tuple $\langle E_1, \ldots, E_n \rangle$ is selected that has exactly W non-zero randomly selected elements from $\mathbb{F}$. Second, a random polynomial p of degree less than k is selected. The public-key is set to $\mathsf{pk} := \{\langle z_i, y_i \rangle\}_{i=1}^n$ where $y_i = p(z_i) + E_i + z_i^k$ for $i = 1, \ldots, n$.
Remark. Observe that $\{\langle z_i, y_i - z_i^k \rangle\}_{i=1}^n$ is a random PR-instance with parameters n, k, W.

The encryption operation is defined with domain $\mathbb{F}^k$ and general range the set $(\mathbb{F} \times \mathbb{F})^n$. The message msg is encoded as a polynomial of degree less than k, denoted by $p_{msg}(x)$; a random tuple $\langle e_1, \ldots, e_n \rangle$ is selected so that it has exactly w non-zero randomly selected field elements; a random element $\alpha \in \mathbb{F}$ is selected as well. The ciphertext that corresponds to msg is the sequence of pairs $\{\langle z_i, y_i' \rangle\}_{i=1}^n$ defined as follows $y_i' = \alpha y_i + p_{msg}(z_i) + e_i$, for $i = 1, \ldots, n$.

So far, the above represents a general approach. The exact choice of parameters (as a function of n, say) gives the specific system of [AF03].

The decryption operates as follows: let $I \subseteq \{1, \ldots, n\}$ be such that $|I| = n - W$ and for all $i \in I$ it holds that $E_i = 0$ (from the selection of the public-key). Observe now that the sequence of pairs $C = \{\langle z_i, y_i' \rangle\}_{i \in I}$ can be seen as a PR-instance with parameters $[n - W, k + 1, w]$. Now suppose that,

$$\text{Condition \#1:} \quad w \leq \frac{n - W - k - 1}{2} \Rightarrow n \geq 2w + W + k + 1$$

This condition implies that the PR-instance has a unique solution that can be recovered by the unique decoding technique of Berlekamp-Welch algorithm. Given such solution $p^*(x)$ it follows that the leading coefficient of p^* will be equal to α (by construction, we have that the polynomial hidden into the public-key is monic and of degree k while the degree of the message polynomial is at most $k-1$). Then, the transmitted message can be recovered as follows $p_{msg}(x) = p^*(x) - \alpha(x^k + p(x))$.

A second condition is that W should be large, beyond the known bounds of list-decoding, to assure that a third party cannot simply get the error locations of the public key (and thus decrypt all ciphertexts). This condition is the base of the presumed security of the scheme.

2.2 A Cryptanalytic Framework

The Cryptanalytic problem that is the basic building block for mounting a ciphertext-only attack on the Public-Key Cryptosystem of [AF03] as described above is defined as follows:

Definition 2. Ciphertext-only Attack Problem *(CAP) Given two sequences of tuples* $X_1 := \{\langle z_i, y_i\rangle\}_{i=1}^n$ *and* $X_2 := \{\langle z_i, y_i'\rangle\}_{i=1}^n$ *and parameters* n, k, w, W *that satisfy the following conditions*

i. $w \leq \frac{n-W-k-1}{2}$ *and* $W \geq n - \sqrt{n(k-1)}$.
ii. $\{\langle z_i, y_i - z_i^k\rangle\}_{i=1}^n$ *is a random PR-instance with parameters* $[n, k, W]$.
iii. $\exists \alpha \in \mathbb{F}$ *such that* $\{\langle z_i, y_i' - \alpha y_i\rangle\}_{i=1}^n$ *is a random PR-instance with parameters* $[n, k, w]$.

Goal. *Find a list of values of polynomial-length that contains the value* α.

Any algorithm that solves CAP in polynomial-time can be turned into a ciphertext-only attack against the cryptosystem of [AF03], as the following proposition reveals.

Proposition 1. *Let* $\mathcal{A}$ *be an algorithm that solves CAP in polynomial-time. Then any message encrypted in the cryptosystem of [AF03] can be decrypted without knowledge of the secret-key in polynomial-time in the security parameter.*

2.3 Coron's Attack

In [Cor03c], Coron presented an elegant ciphertext-only attack against the cryptosystem of [AF03]. We explain the attack briefly below and we show that in fact it can be seen as an algorithm to solve CAP (in fact our formulation of CAP above is motivated by the original attack and by further extensions of this idea in the sequel).

Let X_1, X_2 be an instance of CAP, with $X_1 = \{\langle z_i, y_i\rangle\}_{i=1}^n$ $X_2 = \{\langle z_i, y_i'\rangle\}_{i=1}^n$ and parameters k, w, W, n. Due to condition *iii* of definition 2 it follows that there exist $p \in \mathbb{F}[x]$ of degree less than k and $\alpha \in \mathbb{F}$, so that $p(z_i) \neq y_i' - \alpha y_i$ for at most w indexes i.

The attack modifies the Berlekamp-Welch algorithm: Let $E(x)$ be a monic polynomial of degree w such that $E(z_i) = 0$ for exactly those indexes i for which

$p(z_i) \neq y'_i - \alpha y_i$. The existence of this polynomial is guaranteed due to the condition *iii* of definition 2. Let $N(x) = p(x)E(x)$ be a polynomial of degree less than $k + w$.

Now consider the following system of equations

$$\Big[E(z_i)(y'_i - \lambda y_i) = N(z_i)\Big]_{i=1}^{n} \quad \text{(system 1)}$$

that has as unknowns the $2w+k$ coefficients of the polynomials E, N. Observe that the above system (with λ as a parameter) is not homogeneous (due to the fact that E is monic). Recall that all steps up to this point follow exactly the Berlekamp-Welch algorithm (modulo the unknown λ value).

Now consider the slightly extended system below:

$$\Big[E'(z_i)(y'_i - \lambda y_i) = N(z_i)\Big]_{i=1}^{n} \qquad \text{(system 2)}$$

where $E'(x)$ is a non-monic polynomial that has the same properties as E (i.e. E' and E have the same roots). It follows that system 2 defined above is homogeneous with $2w+k+1$ unknowns. Let $A_2[\lambda]$ be the $n \times (2w+k+1)$-matrix of system 2.

Due to condition i of definition 2 the number of equations n satisfies

$$n \geq 2w + k + 1$$

and thus system 2 has at least as many equations as unknowns.

Case 1 of the Attack. $\text{rank}(A_2[0]) = 2w + k + 1$ (i.e., $A_2[0]$ is of full rank). It follows that there are $2w + k + 1$ linearly independent equations in system 2 for $\lambda = 0$ (and their locations can be recovered e.g. by Gaussian elimination). Without loss of generality let us assume that these are the equations on locations $1, \ldots, 2w + k + 1$. We eliminate the remaining $n - (2w + k + 1)$ equations from system 2, to make it a square homogeneous system, and we call the remaining equations system 3.

It follows that if we substitute the value α for λ in the matrix of the system 3, the matrix is singular since it accepts a solution (the polynomials E', N) that is non-trivial. As a result the matrix of system 3, denoted by $A_3[\lambda]$, has the following property:

$$\exists \alpha \in \mathbb{F} : \det(A_3[\alpha]) = 0$$

Now observe that the determinant of system 3 is a polynomial $f(\lambda) := \det(A_3[\lambda])$ that is of degree at most $w + 1$ (because λ is only involved in the part of the matrix of system 3 that corresponds to the polynomial E').

Further observe that $f(0) = \det(A_3[0]) \neq 0$ because of our selection of $A_3[\lambda]$ to have the property that $A_3[0]$ is the full rank minor of the matrix $A_2[0]$. Thus, the value α is among the $w + 1$ roots of f and the output will be the list of roots of f. It follows that the above algorithm gives an efficient solution for the CAP problem.

Case 2 of the Attack. $\text{rank}(A_2[0]) < 2w + k + 1$. In this case one can find a non-trivial solution of the system $A_2[0]$ which defines two non-zero polynomials E', N such that

$$[E'(z_i)y'_i = N(z_i)]_{i=1}^n$$

Since $y'_i = \alpha(p(z_i) + z_i^k + E_i) + p_{msg}(z_i) + e_i$ it follows that

$$[E'(z_i)(\alpha(p(z_i) + z_i^k + E_i) + p_{msg}(z_i) + e_i) = N(z_i)]_{i=1}^n$$

Let I be the subset of $\{1, \ldots, n\}$ for which it holds that $i \in I \iff (e_i = 0) \wedge (E_i = 0)$. It follows that

$$[E'(z_i)p^*(z_i) = N(z_i)]_{i \in I}$$

where $p^*(x) = \alpha(p(x) + x^k) + p_{msg}(x)$. Recall that the degree of the polynomial N is less than $k + w$ and E' is a polynomial of degree w; it follows that $E'(x)p^*(x)$ is a polynomial of degree $w + k$.

Observe that $|I|$ is a random variable (denoted by η) ranging from $n - w - W$ to $n - \max\{w, W\}$. Next consider this relation:

$$\eta > w + k \quad \text{(Sufficient Condition for Case 2)}$$

Under the above relation, it follows that $|I| \geq w + k + 1$ and as a result the polynomials $E'(x)p^*(x)$ and $N(x)$ are equal. It follows immediately that $p^* = \frac{N}{E'}$; naturally given p^* we recover α immediately and non-ambiguously (in fact, in this case we will even be able to recover the value of the secret-key).

Performing a worst-case analysis of the above, we know that $\eta \geq n - w - W$ and as a result the attack would go through as long as $n-w-W > w+k \iff n > 2w+W+k$ something that matches condition #1 of the [AF03]-cryptosystem (cf. section 2.1) and thus the case 2 of the attack can be carried for the parameters of the cryptosystem (without even taking into account that η would be somewhat larger than its lower bound $n - w - W$).

On the other hand, it would be of interest to us to find a necessary condition for case 2 of the attack (the reason for this will become clear in section 3). This can be found by setting η to its highest possible value and requiring this to be greater than $w + k$: $\eta := n - \max\{w, W\} > w + k$; this is equivalent to:

$$n > w + \max\{w, W\} + k \quad \text{(Necessary condition for Case 2)}$$

3 The Increased Error Case

The cryptosystem of [AF03] mandates that the number of errors introduced by the sender in the formation of the ciphertext is less or equal to $\frac{n-W-k-1}{2}$ (condition #1 of section 2.1), to ensure unique decoding in the reduced PR-instance that is obtained after removing the W locations that contain the errors of the Public-Key.

We observe that the bound on w is unreasonably low, for the following reason: many of the errors introduced by the sender will fall into the error-area of the public-key, and thus they will not affect the decryption operation (i.e., introducing a new error in an already erroneous location is a case where $1 + 1 = 1$).

To see this better, we can think of the sender in the cryptosystem to be playing the following game: he selects w points out of n and randomizes them. Since W of these points will be discarded by the receiver it follows that the number of the good points (out of the total $n - W$ of good points) that will be randomized by the sender follow a *hypergeometric* distribution with mean value $\frac{n-W}{n}$. It follows that the expected number of good points that will be randomized by the sender are $w\frac{n-W}{n}$.

In order to ensure decoding for the decryption operation it suffices to force $\tilde{e} \leq \frac{n-W-k-1}{2}$ where $\tilde{e}$ is a random variable that follows the hypergeometric distribution with mean $\frac{n-W}{n}$. Let $w = \frac{1}{\frac{n-W}{n}+\epsilon}\frac{n-W-k-1}{2}$, for some $\epsilon > 0$. Using the Chvátal bound for the hypergeometric distribution, [Chv79], we have that

$$\mathbf{Prob}[\tilde{e} > (\frac{n-W}{n} + \epsilon)w] \leq e^{-2\epsilon^2 w} \Longrightarrow \mathbf{Prob}[\tilde{e} > \frac{n-W-k-1}{2}] \leq e^{-2\epsilon^2 w}$$

From the above, as long as $\epsilon < W/n$, if we set $w = \frac{1}{\frac{n-W}{n}+\epsilon}\frac{n-W-k-1}{2}$ it follows that the probability $\mathbf{Prob}[\tilde{e} > \frac{n-W-k-1}{2}] \leq e^{-2\epsilon^2 w}$, and thus condition # 1 of section 2.1 will be satisfied in the probabilistic sense and decryption will succeed with probability $1 - e^{-2\epsilon^2 w}$.

We will concentrate on parameters s.t. $W > w$ and w is selected as above. Consider for example the assignment $n = 2000$, $k = 100$, $W \geq 1556$ (to avoid an attack with [GS98] on the public-key), e.g. we set $W = 1600$, and $\epsilon = 1/6$; now observe that $W/n = 0.8 > 1/6$. The equation for w mentioned above yields $w = 407$. It follows that the probability of correct decryption is $1 - e^{-2\frac{407}{36}} = 1 - e^{-22} \approx 1 - 2^{-31}$. Observe now that case 2 of Coron's attack would be foiled since the necessary condition fails:

$$n > w + \max\{w, W\} + k \Longleftrightarrow 2000 > 1600 + 407 + 100 \Longleftrightarrow \mathsf{false}$$

Thus, by merely increasing the number of errors that the sender of the cryptosystem introduces during encryption (relying on randomization to allow decryption with very high probability), we are capable of thwarting the analysis of Coron's attack (in particular the analysis of case 2 of the attack). Observe that this is possible without any other modification of the cryptosystem whatsoever.

Nevertheless, this is only a temporary comfort as we will prove in the next section.

4 With High Probability Modified Coron's Attack Succeeds against Increased Errors

Next, we use another probabilistic analytical tool to show that, in fact, in spite of the increased errors, the attack actually works with high probability.

First, observe the error-increase we introduced in section 3 does not apply to case 1 of Coron's attack. Indeed, one can show for any $\epsilon > 0$ that

$$w = \frac{1}{\frac{n-W}{n} + \epsilon} \frac{n - W - k - 1}{2} \leq \frac{n - k - 1}{2}$$

and the condition $w \leq (n - k - 1)/2$ is sufficient for case 1 to go through (that is, if we can apply it). Recall that case 1 of the attack only applies to the case $\det(A_3[0]) \neq 0$.

We will show that this in fact happens most of the times (a fact observed in practice in [Cor03c] but not proved). This means that the attack works even in the increased error setting of the previous section. Let us recall the matrix of system 2, as defined in section 2.3.

$$A_2[\lambda] = \begin{pmatrix} B_2 \; C_2[\lambda] \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & z_1 & \ldots & z_1^{w+k-1} & y_1' - \lambda y_1 & (y_1' - \lambda y_1)z_1 & \ldots & (y_1' - \lambda y_1)z_1^w \\ 1 & z_2 & \ldots & z_2^{w+k-1} & y_2' - \lambda y_2 & (y_2' - \lambda y_2)z_2 & \ldots & (y_2' - \lambda y_2)z_2^w \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & z_n & \ldots & z_n^{w+k-1} & y_n' - \lambda y_n & (y_n' - \lambda y_n)z_n & \ldots & (y_n' - \lambda y_n)z_n^w \end{pmatrix}$$

where B_2 is a Vandermonde matrix of dimension $w + k$ over the elements $z_1, \ldots, z_n$; B_2 corresponds to the coefficients of $N(x)$; $C_2[\lambda]$ is a Vandermonde matrix of dimension $w + 1$ over the elements $z_1, \ldots, z_n$ where its i-th row is multiplied by $y_i' - \lambda y_i$, for $i = 1, \ldots, n$; C_2 corresponds to the coefficients of $E'(x)$. Recall that $A_2[\lambda]$ is a $n \times (2w + k + 1)$ matrix. We would like to prove that $\mathrm{rank}(A_2[0]) = 2w + k + 1$ with overwhelming probability.

If $\mathrm{rank}(A_2[0]) < 2w + k + 1$ then it follows that any $(2w + k + 1)$-minor of $A_2[0]$ is singular. Below we show that this event can only happen with very small probability (assuming that the underlying finite field $\mathbb{F}$ is large — something that is assumed in [AF03]) thus we deduce that the first case of the attack would work almost always.

Theorem 1. *Let* $\mathbf{P} = \mathbf{Prob}[\mathrm{rank}(A_2[0]) < 2w + k + 1]$ *be the probability that the rank of* $A_2[0]$ *is less than* $2w + k + 1$ *where the probability is taken over all possible choices for the given CAP instance out of which we construct* $A_2[\lambda]$*. It holds that* $\mathbf{P} \leq 2w/|\mathbb{F}|$ *and the proof works even if the first inequality of condition* i *of definition 2 is relaxed to only* $w \leq (n - k - 1)/2$*.*

5 The Most General AF System Avoids Coron's Attack

5.1 An "optimal variant" of the [AF03] cryptosystem

In this section we show that the number of errors w introduced by the sender can, in fact, be increased further beyond the improved bound that we describe in section 3, by employing the proper decoding method for decryption (cf. figure

1). In particular, we make the following crucial observation: [AF03] requires that w is below the error-correction bound of Reed-Solomon Codes, so that the decryption (decoding) is unique. Nevertheless the introduction of random errors in a large enough finite field (such fields are utilized in [AF03]) suggests that uniqueness of decoding can be ensured far beyond the error-correction bound.

In the lemma below we show that randomly selected PR instances that can accept two different decodings are unlikely. This probabilistic analysis allow us to resort to modern list-decoding techniques in the sequel.

Lemma 1. *Let* $\{\langle z_i, y_i\rangle\}_{i=1}^{n}$ *be a RS-Code codeword of a random message* $p \in \mathbb{F}[x]$ *with* $\mathrm{degree}(p) < k$ *that has* e *errors uniformly random distributed over* $\mathbb{F}$*, s.t.* $e < n-k$*. Then, the probability that it accepts another decoding* $p' \in \mathbb{F}[x]$ *with* $p \neq p'$ *is at most* $\binom{n}{t}^2/(|\mathbb{F}|^{n-e-k})$ *(the probability is taken over all possible messages and noise corruptions).*

Now observe that if the "message rate" is $\kappa := k/n$ and the "error-rate" is $\epsilon := e/n$, with $\kappa, \epsilon \in \mathbf{Q}^+$ then it follows that the probability in lemma 1 is less than $\frac{4^n}{|\mathbb{F}|^{(1-\epsilon-\kappa)n}}$. As a result, provided that $\mathbb{F}$ satisfies $|\mathbb{F}|^{1-\epsilon-\kappa} > 4$ it follows that the probability of proposition 1 is "negligible."

Optimal Parameter Setting & Modifications for the Cryptosystem of [AF03]. Taking advantage of the above Lemma in conjunction with the observation of section 3, we can increase the error-parameter w further. We refer to our choice as optimal with respect to figure 1 under the basic assumption that the list-decoding algorithm of [GS98] represents the state of the art in RS-decodability.

Below we assume that the sender employs the algorithm of [GS98] for decryption. For this algorithm to work it should hold that $\tilde{e} < (n-W) - \sqrt{(n-W)k}$ where $\tilde{e}$ is the number of errors introduced in the area of good points of the public-key due to the encryption operation. As argued in section 3, $\tilde{e}$ is a random variable following a hypergeometric distribution with mean $w\frac{n-W}{n}$. In our analysis below we will simply substitute $\tilde{e}$ for the expected number of errors. Note that this does not guarantee that the receiver will be capable of recovering the transmitted message "most of the times." To guarantee this we would have to show that the probability $\mathbf{Prob}[\tilde{e} < (n-W) - \sqrt{(n-W)k}]$ is overwhelming (as we did in section 3), something that cannot simply be inferred from the fact that the mean of $\tilde{e}$ is less than $(n-W) - \sqrt{(n-W)k}$; in order for the receiver to be able to decrypt most of the times we would instead require that the mean of $\tilde{e}$ is sufficiently lower than the bound $(n-W) - \sqrt{(n-W)k}$ and then employ the Chvátal bound on the tails of the hypergeometric distribution to bound the error probability by a negligible fraction, [Chv79] (as in section 3).

Nevertheless, since we intend to cryptanalyze the resulting cryptosystem, we will opt for simply substituting $\tilde{e}$ for its mean, as this would only make our attack stronger. On the other hand observe that a public-key cryptosystem that works, say, half the times is still quite useful. Thus, substituting $\tilde{e}$ for $w\frac{n-W}{n}$ we obtain

$$w\frac{n-W}{n} < (n-W) - \sqrt{(n-W)k} \Longrightarrow w < n - n\sqrt{\frac{k}{n-W}}$$

We conclude that the optimal selection would allow the parameter w to be selected as high as:

$$w < n(1 - \sqrt{\frac{k}{n-W}})$$

The new bound above increases the number of errors that we can allow the sender to introduce, as long as W is selected appropriately:

Proposition 2. *There are choices for W such that $W \geq n - \sqrt{n(k-1)}$ and $n(1 - \sqrt{\frac{k}{n-W}}) > \frac{n-k-1}{2}$, as long as $k \geq 5$ and $k/n \leq 1/16$.*

Now recall that the necessary condition for Coron's attack (both cases) is $w \leq \frac{n-k-1}{2}$. It follows from the proposition above that our analysis puts the parameter w beyond the range of Coron's attack, provided that W is properly selected. To illustrate this concretely, suppose that $n = 2500$ and $k = 101$. Then, W should be selected in the range $[2000, \ldots, 2126]$; if we make the choice $W = 2063$ then we can set w to be as high as 1298, whereas Coron's attack would correct any value of w only up to 1199. Note that the gap of 99 elements between the bound of Coron's attack and the assignment $w = 1298$ ensures that the application of the attack by removing 99 points at random would only succeed with probability less than $(0.52)^{99} \approx 2^{-96}$ (since the ratio of the sender-introduced error points is ≈ 0.52).

Corollary 1. *Coron's attack cannot be applied against the [AF03]-cryptosystem in the optimal parameter setting.*

To draw a parallel to our exposition in section 2.2, we introduce the problem CAP+ to stand for the ciphertext-only attack problem of the optimal variant of Augot and Finiasz Cryptosystem, (the only difference from CAP being in the choice of w):

Definition 3. Ciphertext-only Attack Problem in the optimal parameter setting *(CAP+) Given two sequences of tuples $X_1 := \{\langle z_i, y_i \rangle\}_{i=1}^n$ and $X_2 := \{\langle z_i, y'_i \rangle\}_{i=1}^n$ and parameters k, w, W that satisfy the following conditions*

i. $w < n(1 - \sqrt{\frac{k}{n-W}})$, *and* $W \geq n - \sqrt{n(k-1)}$.
ii. $\{\langle z_i, y_i - z_i^k \rangle\}_{i=1}^n$ *is a random PR-instance with parameters* $[n, k, W]$.
iii. $\exists \alpha \in \mathbb{F}$ *such that* $\{\langle z_i, y'_i - \alpha y_i \rangle\}_{i=1}^n$ *is a random PR-instance with parameters* $[n, k, w]$.

Goal. *Find a list of values of polynomial-length that contains the value α.*

As before we show that any algorithm that solves CAP+ can be used to mount a ciphertext-only attack on the cryptosystem of [AF03] (but now in the optimal parameter setting):

Proposition 3. *Let $\mathcal{A}$ be an algorithm that solves CAP+ in polynomial-time. Then any message encrypted in the cryptosystem of [AF03] in the optimal parameter setting can be decrypted without knowledge of the secret-key in polynomial-time in the security parameter.*

In the Lemma below we give an upper bound on the value of w (that is independent of W).

Lemma 2. *For any CAP+ instance, it holds that $n - w > \sqrt[4]{n^3(k-1)}$.*

6 The Attack Against the General System Employing List-Decoding

The results we present in this section (essentially an algorithm for solving CAP+) is based on Sudan's list-decoding algorithm, [Sud97] and Guruswami Sudan [GS98] algorithms (for both there are efficient polynomial-time algorithms, see [McE03]).

6.1 The attack

Let $n, k, w, W \in \mathbf{Z}$ and $X_1 = \{\langle z_i, y_i\rangle\}_{i=1}^n, X_2 = \{\langle z_i, y_i'\rangle\}_{i=1}^n$ be an instance of CAP+. We denote $\hat{y}_i := y_i' - \lambda y_i$ for $i = 1, \ldots, n$, where λ is an unspecified parameter (free variable); to set the parameter λ to a specific value α we will write $\hat{y}_i[\alpha]$.

According to the definition of a CAP+ instance we know that there exists a value $\alpha \in \mathbb{F}$ (the "encryption coefficient") and a polynomial $p \in \mathbb{F}[x]$ of degree less than k (the "message polynomial") that agrees with $n - w$ of the points $\langle z_i, \hat{y}_i[\alpha]\rangle$. Define $l := n - w - 1$. Next we consider the following system of equations on a set of unknowns $\{q_{j_1,j_2}\}_{j_1\geq 0, j_2\geq 0, j_1+(k-1)j_2<l}$ (called system 4):

$$\forall i \in \{1, \ldots, n\} \qquad \sum_{j_1\geq 0, j_2\geq 0, j_1+(k-1)j_2<l} q_{j_1,j_2} z_i^{j_1} \hat{y}_i^{j_2} = 0 \ \ (\text{system } 4)$$

Observe that any solution to system 4 above defines a bivariate polynomial $Q(x, y)$ that satisfies the property $\text{degree}_{Q,x} + (k-1)\text{degree}_{Q,y} < l$.

Lemma 3. *The number of unknowns of system 4, is at least $\frac{l(l-1)}{2(k-1)}$.*

Recall that from proposition 2 we know that we only consider parameter choices that satisfy $k/n \leq 1/16$. For such range of parameters (and sufficiently large n) we, in fact, show:

Lemma 4. *System 4 is not overdefined provided that $n \geq 19$ and $k/n \leq 1/9$.*

Subsequently we omit the appropriate number of unknowns from system 4, to equalize the number of unknowns and equations. This results in a square homogeneous system of n equations and unknowns that we call system 5. We denote the matrix of system 5 by $A[\lambda]$.

Theorem 2. *Let $\alpha \in \mathbb{F}$ be the "encryption coefficient" for a CAP+ instance as defined in item iii of definition 3. The matrix $A[\alpha]$ as constructed above is singular.*

Since $A[\alpha]$ is singular, it follows that if we define the polynomial $f(\lambda) := \mathrm{Det}(A[\lambda])$, α will be among the solutions of $f(\lambda)$. Thus we can solve CAP+ by computing all the (polynomialy many, by degree constraint) roots of $f(\lambda)$.

Theorem 3. *The probability $\mathbf{P}$ that the polynomial $f(\lambda) = \mathrm{Det}(A[\lambda])$ is the zero-polynomial satisfies $\mathbf{P} \leq 2s(n-l)/|\mathbb{F}|$, where $s = \lfloor \frac{l-1}{k-1} \rfloor$ (the maximum degree of the y-variable in any of the columns of $A[\lambda]$).*

7 Summary

In this section, we summarize our cryptanalytic results.

Given an instance of CAP+ $\{\langle z_i, y_i\rangle\}_{i=1}^n$, $\{\langle z_i, y_i'\rangle\}_{i=1}^n$ with parameters n, k, w, W.
0. Set $l := n - w - 1$.
1. Select $D \subseteq \mathbb{N} \times \mathbb{N}$ so that $\lvert D\rvert = n$ and for all $\langle j_1, j_2\rangle \in D$, $j_1 + (k-1)j_2 < l$
2. Let $\boldsymbol{D} = \left\langle \langle j_1[1], j_2[1]\rangle, \ldots, \langle j_1[n], j_2[n]\rangle \right\rangle$, a lexicographic ordering of D.
3. Construct a $(n \times n)$-matrix A so that its (i, i')-entry equals $z_i^{j_1[i']}(y_i' - \lambda y_i)^{j_2[i']}$
4. Compute $f(\lambda) := \det(A[\lambda])$ symbolically to obtain the polynomial f on λ.
5. Output all roots of f.

Fig. 2. The algorithm that solves CAP+

First in figure 2 we overview the CAP+ algorithm that was presented in the previous section. Using this, the general cryptosystem based on Augot and Finiasz [AF03], even under the optimal choice of parameters is broken under ciphertext-only attacks. The breaking algorithm is summarized in figure 3.

Given the public-key and a ciphertext of the [AF03]-cryptosystem with parameters n, k, w, W.
1. if $w \leq \frac{n-k-1}{2}$ invoke case 1 of Coron's attack.
2. else invoke the CAP+ algorithm of figure 1, and recover the plaintext using Guruswami-Sudan algorithm (as described in proposition 3).

Fig. 3. The attack against the Generalized Version of [AF03]-Cryptosystem.

Note that the attack outlined above is probabilistic and is guaranteed to work with very high probability as we have shown in theorem 1 (for case 1 of Coron's attack), and theorem 3 (for CAP+ algorithm).

References

[AF03] Daniel Augot and Matthieu Finiasz, *A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem*, Eli Biham (Ed.): Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings. Lecture Notes in Computer Science 2656 Springer 2003, pp. 229-240.

[AFL03] Daniel Augot, Matthieu Finiasz and Pierre Loidreau, *Using the Trace Operator to repair the Polynomial Reconstruction based Cryptosystem presented at Eurocrypt 2003*, Cryptology ePrint Archive, Report 2003/209, 2003, `http://eprint.iacr.org/`.

[BW86] Elwyn R. Berlekamp and L. Welch, *Error Correction of Algebraic Block Codes.* U.S. Patent, Number 4,633,470, 1986.

[Chv79] Vasek Chvátal, *The tail of the hypergeometric distribution*, Discrete Math, Vol. 25, pp. 285-287, 1979.

[Cor03a] Jean-Sebastien Coron, *Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem*, Cryptology ePrint Archive, Report 2003/036. `http://eprint.iacr.org/`.

[Cor03b] Jean-Sebastien Coron, *Cryptanalysis of the Repaired Public-key Encryption Scheme Based on the Polynomial Reconstruction Problem*, Cryptology ePrint Archive, Report 2003/219. `http://eprint.iacr.org/`.

[Cor03c] Jean-Sebastien Coron, *Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem*, in Feng Bao, Robert H. Deng, Jianying Zhou (Eds.): Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004. Lecture Notes in Computer Science 2947 Springer 2004, pp. 14-27.

[GS98] Venkatesan Guruswami and Madhu Sudan, *Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes.* In the Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, California, November 8-11, IEEE Computer Society, pp. 28–39, 1998.

[KY02] Aggelos Kiayias and Moti Yung, *Cryptographic Hardness based on the Decoding of Reed-Solomon Codes*, in the Proceedings of ICALP 2002, Lecture Notes in Computer Science, vol. 2380, Malaga, Spain, July 8-13, pp. 232-243.

[KY04] Aggelos Kiayias and Moti Yung, *Cryptanalyzing the Polynomial-Reconstruction based Public-Key System Under Optimal Parameter Choice*, Cryptology ePrint Archive, Report 2004/217. `http://eprint.iacr.org/`.

[McE78] Robert J. McEliece. *A public key cryptosystem based on algebraic coding theory. Jet Propulsion Lab, DSN Progress Report*, 42(44), pp. 114–116, Jan-Feb 1978.

[McE03] Robert J. McEliece, The Guruswami-Sudan Decoding Algorithm for Reed-Solomon Codes, IPN Progress Report 42-153, May 15, 2003. `http://ipnpr.jpl.nasa.gov/tmo/progress_report/42-153/153F.pdf`.

[Sch80] Jacob T. Schwartz, *Fast Probabilistic Algorithms for Verifications of Polynomial Identities*, Journal of the ACM, Vol. 27(4), pp. 701–717, 1980.

[Sud97] Madhu Sudan, *Decoding of Reed Solomon Codes beyond the Error-Correction Bound.* Journal of Complexity 13(1), pp. 180–193, 1997.