

Cryptanalysis of the the Polynomial Reconstruction Based Public-Key Cryptosystem of Eurocrypt'03 in the Optimal Parameter Setting

Aggelos Kiayias

Computer Science & Engineering
University of Connecticut
Storrs, CT, USA
aggelos@cse.uconn.edu

Moti Yung

Computer Science
Columbia University
New York, NY, USA
moti@cs.columbia.edu

Abstract

In Eurocrypt 2003, Augot and Finiasz presented a novel Public-key Cryptosystem based on the Polynomial Reconstruction Problem. While there is no immediate way to use coding theoretic techniques to break their system, it has been subsequently broken by Coron who presented a ciphertext-only attack (based on a worst case analysis).

In the present work we study the optimal parameter setting of their cryptosystem and analyze it from a probabilistic point of view. We first show that a small modification of the parameters of this scheme foils the worst case analysis of the above attack; however we give an alternative probabilistic analysis showing that the attack works almost always. We then present a novel analysis of optimal parameter selection for their cryptosystem. We show that in the optimal setting of parameter selection, the Augot and Finiasz cryptosystem actually thwarts Coron's attack. Then, we present a stronger ciphertext-only attack based on the Sudan and Guruswami-Sudan's list-decoding algorithms that breaks the optimal parameter setting of this cryptosystem. We conclude that the Augot and Finiasz's cryptosystem, regardless of exact choice of parameters, succumbs to a polynomial-time ciphertext-only attack.

1 Introduction.

Polynomial Reconstruction 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 tuples $\{(z_i, y_i)\}_{i=1}^n$, 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 indices $i \in \{1, \dots, n\}$.*

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. 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).

Based on this last remark, the PR and related problems have been employed in the cryptographic setting as intractability assumptions. In particular, a related problem to PR was put forth by Naor and Pinkas [NP99] to base the security of their “Oblivious Polynomial Evaluation” protocol on; this setting was extended in [KY01]. Subsequently, in [KY02], Kiayias and Yung investigated several properties and basic cryptographic primitives that can be built directly over Polynomial Reconstruction instances, including a semantically secure symmetric key cipher.

Recently, in Eurocrypt 2003 [AF03], Augot and Finiasz presented a public-key cryptosystem that was based on PR. Their approach 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 approach allows key sizes that are much smaller than the traditional coding theoretic based public-key systems. Further, direct use of the above mentioned decoding and list-decoding methods do not apply to breaking the cryptosystem (directly).

However, the scheme has been recently broken by Coron [Cor03] (without affecting the solvability of PR). The attack presented in [Cor03] 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.

In the present work, we investigate the optimization of the parameter selection in the Augot and Finiasz cryptosystem and in particular of the number of errors that are introduced by the sender during encryption. Arguably this is the most sensitive parameter in the cryptosystem. Regarding the optimization (maximization) of this parameter we make two key-observations (1) [AF03] employ a worst-case approach in selecting this parameter; a probabilistic approach (that we perform in this work) allows higher values. (2) [AF03] employ regular RS-decoding for the decryption operation; we emphasize that more powerful decoding techniques can be employed that allow larger values for the parameter.

Regarding our key-observation (1) we employ the tails of the hypergeometric distribution to show that the original cryptosystem allows too few errors to be used by the message encryption process when adding the second PR instance (the one corresponding to the message). Thus the sender error-parameter can be increased high enough to partially fail the attack analysis given by Coron. Nevertheless we provide an alternative probabilistic analysis showing that Coron’s attack would work almost always even in this slightly modified (more noisy) version.

Combining our key-observations (1) and (2) we discover the optimal setting for the sender error-parameter (“optimal” under the assumption that the Guruswami-Sudan list-decoding algorithm represents the best possible decoding algorithm against Polynomial Reconstruction) and we show that Coron’s attack can be totally thwarted in this case. Then, we present a

new attack that is based on the Sudan and Guruswami-Sudan’s algorithm that breaks even the optimal parameter setting.

Methodologically, our approach relies on designing and analyzing the schemes from the “probabilistic method” perspective, while at the same employing the state-of-the art in Reed-Solomon Codes algorithmic decodability.

Finally, we remark that Coron’s attack [Cor03] totally breaks the cryptosystem of Augot and Finiasz as published in [AF03]. The contribution of the present work is to show that the [AF03] is insecure even if its parameters are selected optimally.

2 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 $p_{msg}(x) = p^*(x) - \alpha p(x)$.

In more detail, let $z_1, \dots, z_n \in \mathbb{F}$ 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 $\langle E_1, \dots, E_n \rangle$ 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 $\mathbf{pk} := \{\langle z_i, y_i \rangle\}_{i=1}^n$ where $y_i = p(z_i) + E_i + z_i^k$ for $i = 1, \dots, n$.

Remark 1. 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 $\langle e_1, \dots, e_n \rangle$ 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 $i = 1, \dots, n$.

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 $I \subseteq \{1, \dots, n\}$ 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 $[n - W, k + 1, w]$. It follows that given the condition

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

This condition implies that the PR-instance has a unique solution that can be recovered by the Berlekamp-Welch algorithm. Given such solution $p^*(x)$ it follows (by construction) that the leading coefficient of p^* will be equal to α . 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.

3 A Cryptanalytic Framework

The Cryptanalytic problem that is the basic building block for mounting a ciphertext-only attack on a 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 3 *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.*

Proof. Observe that due to the definition of the cryptosystem the condition *i* of definition 2 is satisfied. Also if we set the public-key to be X_1 and the ciphertext to be X_2 it follows that conditions *ii, iii* of definition 2 are also satisfied. Thus, we can apply (simulate) \mathcal{A} on X_1, X_2 to obtain α . Now observe that due to conditions *iii* and *i* we can decode $\{\langle z_i, y'_i - \alpha y_i \rangle\}_{i=1}^n$ (using the Berlekamp-Welch algorithm) to obtain the transmitted message $p_{msg}(x)$ (unique solution). \mathcal{A} guarantees polynomially many candidates for α , thus the above reduction will be successful in returning the plaintext with probability at most $1/\text{poly}$. \square

4 Coron's Attack

In [Cor03], Coron presented a 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 $X_1 = \{z_i, y_i\}_{i=1}^n$ $X_2 = \{z_i, y'_i\}_{i=1}^n$ 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 indices 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 indices 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

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

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). Observe that all steps up to this point are exactly the Berlekamp-Welch algorithm (modulo the unknown λ value).

Now consider the slightly extended system below:

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

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 $1, \dots, 2w + k + 1$. 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 $\{1, \dots, n\}$ 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) 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 a 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 5). 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:

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

5 A Straightforward Error Increase Scheme Avoids Coron's Analysis

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 $\frac{n-W-k-1}{2}$, 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. 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

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

Observe that 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 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:

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

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.

6 Coron's Attack Succeeds with Increased Errors

First, observe the error-increase we introduced in section 5 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, using probabilistic analysis, that this in fact happens most of the times (a fact observed in practice in [Cor03] but not proven). 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 4.

$$A_2[\lambda] = \begin{pmatrix} B_2 & C_2[\lambda] \end{pmatrix} = \begin{pmatrix} 1 & z_1 & \dots & z_1^{w+k-1} & y'_1 - \lambda y_1 & (y'_1 - \lambda y_1)z_1 & \dots & (y'_1 - \lambda y_1)z_1^w \\ 1 & z_2 & \dots & z_2^{w+k-1} & y'_2 - \lambda y_2 & (y'_2 - \lambda y_2)z_2 & \dots & (y'_2 - \lambda y_2)z_2^w \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & z_n & \dots & z_n^{w+k-1} & y'_n - \lambda y_n & (y'_n - \lambda y_n)z_n & \dots & (y'_n - \lambda y_n)z_n^w \end{pmatrix}$$

where B_2 is a Vandermonde matrix of dimension $w + k$ over the elements z_1, \dots, z_n ; B_3 corresponds to the coefficients of $N(x)$; $C_2[\lambda]$ is a Vandermonde matrix of dimension $w + 1$ over the elements z_1, \dots, z_n where its i -th row is multiplied by $y'_i - \lambda y_i$, for $i = 1, \dots, n$; 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 $\text{rank}(A_2[0]) = 2w + k + 1$ with overwhelming probability.

If $\text{rank}(A_2[0]) < 2w + k + 1$ 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 4 *Let $\mathbf{P} = \mathbf{Prob}[\text{rank}(A_2[0]) < 2w + k + 1]$ 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 we the first inequality of condition i of definition 2 is relaxed to only $w \leq (n - k - 1)/2$.*

Proof. First observe that due to the conditions i of definition 2 it holds that $W > w$ (even under the relaxation $w \leq (n - k - 1)/2$). Suppose that the selection of the error-locations for a CAP instance is denoted by \vec{r} . Let $J_{\vec{r}}$ be a subset of $\{1, \dots, n\}$ such that $|J_{\vec{r}}| = 2w + k + 1$ and J overlaps with all elements $i \in \{1, \dots, n\}$ that have the property $e_i \neq 0$, as well as at least one element $i_0 \in \{1, \dots, n\}$ with the property $e_{i_0} = 0$ but $E_{i_0} \neq 0$ (the existence of i_0 is assured by the fact $W > w$). Let us now define a minor $M_{\vec{r}}$ of $A_2[0]$

$$M_{\vec{r}} = \left(1 \quad z_i \quad \dots \quad z_i^{w+k-1} \quad y'_i \quad y'_i z_i \quad \dots \quad y'_i z_i^w \right)_{i \in J_{\vec{r}}}$$

We will show that for any \vec{r} , $M_{\vec{r}}$ is of full rank with very high probability over the remaining coin-tosses that sample a CAP instance (even in the relaxed setting $w \leq (n - k - 1)/2$). Recall that we have that $y'_i = \alpha y_i + p_{msg}(z_i) + e_i$ where $p_{msg}(x) \in \mathbb{F}[x]$ is a polynomial of degree less than k and $\langle e_1, \dots, e_n \rangle$ is a tuple of Hamming weight w . Also that, $y_i = p(z_i) + E_i + z_i^k$, where $\langle E_1, \dots, E_n \rangle$ is a random tuple of Hamming weight W . It follows that every column among the $w + 1$ rightmost columns of $M_{\vec{r}}$ can be written as

$$col_j := \langle \alpha z_i^j ((p(z_j) + E_i + z_i^k) + p_{msg}(z_i) + e_i) \rangle_{i \in J_{\vec{r}}} \quad j = 0, \dots, w$$

Now observe that we can view $\det(M_{\vec{r}})$ as a multivariate polynomial on the variables

$$\alpha, e_1, \dots, e_n, E_1, \dots, E_n, a_0, \dots, a_{k-1}, b_0, \dots, b_{k-1}$$

where a_0, \dots, a_{k-1} are the coefficients of $p(x)$ and b_0, \dots, b_{k-1} are the coefficients of $p_{msg}(x)$. These variables are either free, or bound to be 0 (e.g. if randomness \vec{r} dictates that i' is not among the error-locations of the public-key it holds that $E_{i'}$ is bound to be 0).

Without loss of generality we may assume that \vec{r} and $J_{\vec{r}}$ are selected so that e_1, \dots, e_w, E_{w+1} are free variables (i.e. correspond to random error-locations); note that any other possibility would work in the same way. Now let us consider the following assignment to the multi-variate polynomial $\det(M_{\vec{r}})$:

$$(\alpha = 1, e_1 = z_1^{w+k}, \dots, e_w = z_w^{w+k}, E_1 = 0, \dots, E_w = 0, E_{w+1} = z_{w+1}^{w+k}, E_{w+2} = 0, \dots, E_W = 0, a_0 = 0, \dots, a_{k-1} = 0, b_0 = 0, \dots, b_{k-1} = 0) =$$

It follows that $\det(M_{\vec{r}})$ takes the following value:

$$\begin{vmatrix} 1 & z_1 & \dots & z_1^{w+k-1} & z_1^{w+k} & z_1^{w+k+1} & \dots & z_1^{2w+k} \\ 1 & z_2 & \dots & z_2^{w+k-1} & z_2^{w+k} & z_2^{w+k+1} & \dots & z_2^{2w+k} \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & z_{w+1} & \dots & z_{w+1}^{w+k-1} & z_{w+1}^{w+k} & z_{w+1}^{w+k+1} & \dots & z_{w+1}^{2w+k} \\ 1 & z_{w+2} & \dots & z_{w+2}^{w+k-1} & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & z_{2w+k+1} & \dots & z_{2w+k+1}^{w+k-1} & 0 & 0 & \dots & 0 \end{vmatrix}$$

The above determinant is non-zero (it can be seen easily as an application of well-known properties of Vandermonde matrices), and as a result the multivariate polynomial $\det(M_{\vec{r}})$ is not the zero-polynomial. It follows from Schwartz's Lemma, [Sch80], that the ratio of the roots of the non-zero multivariate polynomial $\det(M_{\vec{r}})$ is bounded from above by τ/\mathbb{F} where $\tau \leq 2w$ is the total degree of $\det(M_{\vec{r}})$. \square

7 An Optimal Approach Thwarts Coron's Attack

7.1 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 5, with some slight modifications to the decryption function. 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 field (such fields are utilized in [AF03]) suggests that uniqueness of decoding can be ensured far beyond the error-correction bound: see e.g. [KY02] for an explicit proof of this fact. This suggests that decoding of random PR-instances can be done uniquely using decoding algorithms that go beyond the error-correction bound of RS-codes, i.e. the Guruswami-Sudan algorithm.

Optimal Parameter Setting & Modifications for the Cryptosystem of [AF03]. Taking advantage of the above fact in conjunction to the observation of section 5, we can increase the error-parameter w further. We refer to our choice as optimal 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 to the area of good points of the public-key due to the encryption operation. As argued in section 5, \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 5), 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 5). 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

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

We conclude that the optimal upper bound for the parameter w is:

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

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 5 *There are choices for W such that $W \geq n - \sqrt{n(k - 1)}$ and $n \left(1 - \sqrt{\frac{k}{n - W}} \right) > \frac{n - k - 1}{2}$, as long as $k \geq 5$ and $k/n \leq 1/16$. A strict upper bound for k/n is $1/11$.*

Proof. The first inequality $W \geq n - \sqrt{n(k - 1)}$ can be written as $\frac{W}{n} \geq 1 - \sqrt{\frac{k - 1}{n}}$ and it provides a lower bound for W/n . We will see that the second inequality yields an upper bound for W/n :

indeed, $n(1 - \sqrt{\frac{k}{n-W}}) > \frac{n-k-1}{2}$ can be rewritten as $\frac{n+k+1}{2} > n\sqrt{\frac{k}{n-W}}$; to satisfy this latter inequality it suffices to provide a W that satisfies $n+k > 2n\sqrt{\frac{k}{n-W}}$, or $(n-W)(n^2+2nk+k^2) > 4n^2k$. The latter inequality is equivalent to $n(n^2 - 2nk + k^2) > W(n+k)^2$ or $\frac{W}{n} < \frac{(n-k)^2}{(n+k)^2}$.

$$\frac{(n-k)^2}{(n+k)^2} = \frac{n^2 + k^2 + 2nk - 4nk}{n^2 + k^2 + 2nk} = 1 - \frac{4nk}{(n+k)^2} = 1 - 4\frac{k/n}{(1+k/n)^2}$$

It follows that we must show,

$$\begin{aligned} 1 - 4\frac{k/n}{(1+k/n)^2} > 1 - \sqrt{\frac{k-1}{n}} &\iff \sqrt{\frac{k-1}{n}} > 4\frac{k/n}{(1+k/n)^2} \iff (1+k/n)^4 \frac{k-1}{n} > 16(k/n)^2 \\ &\iff (n+k)^4(k-1) > 16n^3k^2 \iff \frac{(n+k)^4}{n^3} > 16\frac{k^2}{k-1} \end{aligned}$$

Given that $k \geq 5$ we deduce that $20k \geq 16\frac{k^2}{k-1}$, thus it suffices to show that $(n+k)^4 > 20n^3k$, which is equivalent to $n^4 - 16n^3k + 6n^2k^2 + 4nk^3 + k^4 > 0$ which is true provided that $k/n \geq 1/16$.

Observe that if k is very large it holds that $\frac{k^2}{k-1} \approx k$; thus we derive that if $\kappa := k/n$ it holds that κ should satisfy $\kappa^4 + 4\kappa^3 + 6\kappa^2 - 12\kappa + 1 > 0$; as an equation the left-hand-side has two real roots, $\kappa = 1$ and $\kappa \approx 0.0873$; it follows that an upper bound for κ is $1/11$. \square

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 $n = 2000$ and $k = 101$. Then, W should be selected in the range $[2000, \dots, 2126]$; 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 $(0.52)^{99}$ (since the ratio of the sender-introduced error points is ≈ 0.52).

Corollary 6 *Coron's attack fails to break the [AF03]-cryptosystem in the optimal parameter setting.*

To draw a parallel to our exposition in section 3, we introduce the problem CAP+ to stand for the ciphertext-only attack problem of the optimal variant of Augot and Finiasz Cryptosystem, to be called CAP+ (the only difference from CAP being in the choice of w):

Definition 7 Ciphertext-only Attack Problem in the optimal parameter setting (CAP+) *Given two sequences of tuples $X_1 := \{z_i, y_i\}_{i=1}^n$ and $X_2 := \{z_i, y'_i\}_{i=1}^n$ and parameters k, w, W that satisfy the following conditions*

$$i. \ w < n(1 - \sqrt{\frac{k}{n-W}}), \text{ and } W \geq n - \sqrt{n(k-1)}.$$

$$ii. \ \{z_i, y_i - z_i^k\}_{i=1}^n \text{ is a random PR-instance with parameters } [n, k, W].$$

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 8 *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.*

Proof. Similar to the proof of proposition 8 with the difference that now Guruswami-Sudan's algorithm, [GS98], should be employed instead of the Berlekamp-Welch algorithm. \square

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

Lemma 9 *For any CAP+ instance, it holds that $n - w > \sqrt[4]{n^3(k-1)}$.*

Proof. First observe that $n - W \leq n\sqrt{\frac{k-1}{n}} \implies \sqrt{\frac{k-1}{n-W}} \geq \sqrt[4]{\frac{k-1}{n}}$. Since $w < n - n\sqrt{\frac{k}{n-W}} \implies n - w > n\sqrt{\frac{k}{n-W}} > n\sqrt{\frac{k-1}{n-W}} \geq n\sqrt[4]{\frac{k-1}{n}} = \sqrt[4]{n^3(k-1)}$. \square

8 Breaking the Optimal Variant of the [AF03]-cryptosystem

The attack (essentially an algorithm for solving CAP+) is based on Sudan's list-decoding algorithm, [Sud97]. Applications of the enhanced techniques of Guruswami and Sudan, [GS98], are also possible, however unnecessary in our range of parameters.

8.1 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 $i = 1, \dots, n$, 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):

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

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

Proof. The number of unknowns can be easily seen to be equal to the following double sum:

$$\begin{aligned}
& \sum_{j_2=0}^{\lfloor \frac{l-1}{k-1} \rfloor} \sum_{j_1=0}^{l-1-j_2(k-1)} 1 = \sum_{j_2=0}^{\lfloor \frac{l-1}{k-1} \rfloor} (l - j_2(k-1)) = \\
& = l(\lfloor \frac{l-1}{k-1} \rfloor + 1) - (\lfloor \frac{l-1}{k-1} \rfloor + 1) \lfloor \frac{l-1}{k-1} \rfloor \frac{k-1}{2} = (\lfloor \frac{l-1}{k-1} \rfloor + 1) (l - \lfloor \frac{l-1}{k-1} \rfloor \frac{k-1}{2}) \geq \\
& \geq (\frac{l-1}{k-1}) (l - \frac{l-1}{k-1} \frac{k-1}{2}) = \frac{l(l-1)}{2(k-1)}
\end{aligned}$$

□

Recall that from proposition 5 we know that we only consider parameter choices that satisfy $k/n < 1/11$. For such range of parameters (and sufficiently large n) we, in fact, show:

Lemma 11 *System 4 is not overdefined provided that $n \geq 19$ and $k/n \leq 1/9$.*

Proof. In order for system 4 to be not overdefined it suffices to show that,

$$\frac{l(l-1)}{2(k-1)} = \frac{(n-w-1)(n-w-2)}{2(k-1)} \geq n$$

This can be satisfied provided that

$$(n-w-1)(n-w-2) \geq 2(k-1)n \iff (n-w)^2 \geq 2(k-1)n - 2 + 3(n-w)$$

Now observe that, $\frac{2}{3}(n-w)^2 \geq 2(k-1)n$. Indeed $(n-w)^2 > \sqrt{n^3(k-1)}$ (from lemma 9), and it holds that

$$\sqrt{n^3(k-1)} \geq 3(k-1)n \iff \frac{k-1}{n} \leq \frac{1}{9}$$

which is true for our range of parameters.

Next consider the inequality $\frac{1}{3}(n-w)^2 \geq 3(n-w)$; it is equivalent to $n-w \geq 9$ which will be satisfied as long as $\sqrt[4]{n^3(k-1)} \geq 9$ which is true for $n \geq 19$.

We conclude that

$$(n-w)^2 = \frac{2}{3}(n-w)^2 + \frac{1}{3}(n-w)^2 \geq 2(k-1)n + 3(n-w) \geq 2(k-1)n - 2 + 3(n-w)$$

which completes the proof. □

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 12 *Let $\alpha \in \mathbb{F}$ be the “encryption coefficient” for a CAP+ instance as defined in item iii of definition 7. The matrix $A[\alpha]$ as constructed above is singular.*

Proof. Let $\alpha \in \mathbb{F}, p \in \mathbb{F}[x]$ be the solution of the CAP+ instance.

Recall that of the n points $\{(z_i, \hat{y}_i[\alpha])\}_{i=1}^n$, at least $n - w$ of them belong the graph of the polynomial p , which is of degree less than k .

Let i_0 be one of these points and consider the system that results after removing from system 5 the equation below:

$$\sum_{j_1 \geq 0, j_2 \geq 0, j_1 + (k-1)j_2 < l} z_{i_0}^{j_1} \hat{y}_{i_0}^{j_2} = 0$$

We will call the resulting system that has one equation less, “system 6.” It is immediate that system 6 is an underspecified homogeneous system. It follows that it accepts a non-trivial solution.

Now observe that any non-trivial solution to system 6 defines a bivariate polynomial $R \in \mathbb{F}[x, y]$ that has the following properties:

1. R is of degrees d_x, d_y that satisfy $d_x + (k - 1)d_y < l$.
2. For any point $i \neq i_0$, such that $p(z_i) = \hat{y}_i[\alpha]$, it holds that $(x - z_i)$ divides $R(x, p(x))$.
3. It holds that $y - p(x)$ divides $R(x, y)$ (when $R(x, y)$ is viewed as a univariate polynomial on y with coefficients in $\mathbb{F}[x]$).

Justification for Item 1. it follows from the definition of system 4: the degrees of any monomial $x^{j_1}y^{j_2}$ of R satisfy $j_1 + (k - 1)j_2 < l$.

Justification for item 2. Since $p(z_i) = \hat{y}_i[\alpha]$ it follows that z_i is a root of $R(x, p(x))$ and as a result $(x - z_i)$ divides R .

Justification for item 3. Observe that the degree of $R(x, p(x))$ is strictly less than $l = n - w - 1$ (by item 1). We have $n - w - 1$ points among the $\{1, \dots, n\} - \{i_0\}$ that agree with $p(x)$. Using item 2, it follows that $(x - z_i)$ divides $R(x, p(x))$ for $n - w - 1$ points. As a result the degree of $R(x, p(x))$ is at least $n - w - 1 (= l)$, a contradiction, unless $R(x, p(x))$ is exactly the zero-polynomial, something that implies that $y - p(x)$ is a factor of $R(x, y)$ when the latter is seen as a univariate polynomial on y over $\mathbb{F}[x]$.

To complete the proof now observe the following: because of item 3 above it follows that $R(z_{i_0}, p(z_{i_0})) = 0$, and thus the equation that we omitted in order to construct system 6 from system 5 is also satisfied. This means that the solution R to system 6 is also a solution to the extended system 5, and since $R \neq 0$ it follows that system 5 for $\lambda = \alpha$ has a non-trivial solution, thus it holds that $A[\alpha]$ is singular. \square

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

Theorem 13 *The probability \mathbf{P} that the polynomial $f(\lambda) = \text{Det}(A[\lambda])$ 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 $A[\lambda]$).*

Proof. First observe that due to condition i of definition 7 it holds that $W > w$.

Let us examine first the matrix of system 4.

$$A_4[\lambda] = \begin{pmatrix} 1 & z_1 & \dots & z_1^{l-1} & \hat{y}_1 & \hat{y}_1 z_1 & \dots & \hat{y}_1 z_1^{l-1-(k-1)} & \dots & \hat{y}_1^s & \hat{y}_1^s z_1 & \dots & \hat{y}_1^s z_1^{l-s(k-1)} \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ 1 & z_n & \dots & z_n^{l-1} & \hat{y}_n & \hat{y}_n z_n & \dots & \hat{y}_n z_n^{l-1-(k-1)} & \dots & \hat{y}_n^s & \hat{y}_n^s z_n & \dots & \hat{y}_n^s z_n^{l-s(k-1)} \end{pmatrix}$$

Observe that the matrix of system 5, $A[\lambda]$ results from the above matrix by removing a number of columns so that it becomes square. Since $f(\lambda) = \det(A[\lambda])$ it follows that the probability that $f = 0$ is bounded from above from the probability that $\det(A[0]) = 0$. Observe that $A[0]$ is a matrix as above with \hat{y}_i substituted for y'_i (the ciphertext values) for all $i = 1, \dots, n$ (and of course a number of columns removed so that it becomes square).

Let u be some parameter to be specified later. We set $y'_i = z_i^l$ for all $i = 1, \dots, u$ and $y'_i = 0$ otherwise.

Observe that all columns of $A[0]$ are of the form $\langle z_i^{j_1} (y'_i)^{j_2} \rangle_{i=1}^n$ with $j_1 + (k-1)j_2 < l$. Setting $y'_i = z_i^l$ for $i = 1, \dots, u$ it follows that $z_i^{j_1} (y'_i)^{j_2} = z_i^{j_1 + j_2 l}$. Observe now that for all j_1, j_2, j'_1, j'_2 with $j_1 + (k-1)j_2 < l$ and $j'_1 + (k-1)j'_2 < l$ it holds that it cannot be the case that $j_1 + j_2 l = j'_1 + j'_2 l$, unless $\langle j_1, j_2 \rangle = \langle j'_1, j'_2 \rangle$. Assume $j_1 + j_2 l = j'_1 + j'_2 l$. Since $j_1, j'_1 < l$ always it follows that $j_1 = j'_1$; as a result $l j_2 = l j'_2$, but this implies that $j_2 = j'_2$ also.

It follows that the first u rows of $A[0]$ with the substitution $y'_i = z_i^l$ constitute an extended punctured Vandermonde matrix¹ of dimensions $(u \times n)$. The remaining rows of this matrix are of the form

$$\begin{pmatrix} 1 & z_{u+1} & \dots & z_{u+1}^{l-1} & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & z_n & \dots & z_n^{l-1} & 0 & 0 & \dots & 0 \end{pmatrix}$$

We make the selection $u = n - l$. It follows that the above matrix is of full rank. Also the first u rows of $A[0]$ with the substitution $y'_i = z_i^l$ are also of full rank.

The above arguments suggest that there is a way to control the coin tosses of the sender in the cryptosystem so that the matrix $A[0]$ becomes non-singular. To do this we were required to control u error-points. Since $l = n - w - 1$, it holds that $u = n - l = w + 1$. As a result it suffices that we control one additional error-location which happens always since $W > w$ (following similar arguments as in the proof of theorem 4).

With a similar arguments as in the proof of theorem 4 we conclude that using Schwartz Lemma the probability \mathbf{P} that $A[0]$ will be singular satisfies, $\mathbf{P} \leq 2s(n-l)/|\mathbb{F}|$. This concludes the proof. \square

Below we summarize the algorithm that we introduced in this section:

9 Conclusions

We have shown that the cryptosystem of Augot and Finiasz [AF03], even under the optimal choice of parameters is broken under ciphertext-only attacks. The breaking algorithm can be summarized in the following algorithm:

¹we call a matrix M , “extended punctured Vandermonde” if there is a $D \subseteq \mathbb{N}$ and z_1, \dots, z_v pairwise distinct elements of \mathbb{F} , so that M ’s columns are of the form $\langle z_1^d, \dots, z_v^d \rangle^T$ for each $d \in D$. Such matrices are of full rank.

<p>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.</p> <ol style="list-style-type: none"> 0. Set $l := n - w - 1$. 1. Select $D \subseteq \mathbb{N} \times \mathbb{N}$ so that $D = n$ and for all $\langle j_1, j_2 \rangle \in D$, $j_1 + (k - 1)j_2 < l$. 2. Let $\vec{D} = \langle \langle j_1[1], j_2[1] \rangle, \dots, \langle j_1[n], j_2[n] \rangle \rangle$, a lexicographic ordering of D. 3. Construct a $(n \times n)$-square 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.

Figure 1: The algorithm that solves CAP+

<p>Given the public-key and a ciphertext of the [AF03]-cryptosystem with parameters n, k, w, W.</p> <ol style="list-style-type: none"> 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 8).
--

Figure 2: The attack against the Generalized Version of [AF03]-Cryptosystem.

Note that the above general attack is probabilistic and is guaranteed to work with very high probability as we have shown in theorem 4 (for case 1 of Coron's attack), and theorem 13 (for CAP+ algorithm).

Acknowledgement

We wish to thank Daniel Augot, Jean-Sebastian Coron and Matthieu Finiasz for making their results available to us.

References

- [AF03] Daniel Augot and Matthieu Finiasz, *A Public Key Encryption Scheme Based on the Polynomial Reconstruction Problem*, to appear in the proceedings of EUROCRYPT 2003.
- [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.
- [Cor03] Jean-Sebastien Coron, *Cryptanalysis of a public-key encryption scheme based on the polynomial reconstruction problem*, IACR E-print Tech. Report 2003/036.
- [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, IEEE Computer Society, pp. 28-39, 1998.

- [KY01] Aggelos Kiayias and Moti Yung, *Secure Games with Polynomial Expressions*, In the Proceedings of ICALP 2001, LNCS Vol. 2076, pp. 939-950, Springer 2001.
- [KY02] Aggelos Kiayias and Moti Yung, *Cryptographic Hardness based on the Decoding of Reed-Solomon Codes*, in the Proceedings of ICALP 2002, LNCS vol. 2380, pp. 232-243. (See also Electronic Colloquium of Computational Complexity Report TR02-017).
- [NP99] Moni Naor and Benny Pinkas, *Oblivious Transfer and Polynomial Evaluation*. In the Proceedings of the 31th ACM Symposium on the Theory of Computing, 1999.
- [Sch80] J. 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.