Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88

Jacques PATARIN
CP8 TRANSAC, 68 route de Versailles, BP 45 - 78430 Louveciennes Cedex - France

Abstract

In [1] Matsumoto and Imai have developed a new public key scheme for enciphering or signing. (This scheme is completely different and should not be mistaken with another scheme of Matsumoto and Imai developed in 1983 and broken at Eurocrypt'84).
No attacks have been published as yet for this scheme. However we will see in this paper that for almost all the keys almost each cleartext can be found from his ciphertext after only about $m^2n^4 \log n$ computations where m is the degree of the field K chosen, and where mn is the number of bits of the text.
Moreover for absolutely all the keys that give a practical size for the messages it will be possible to find almost all the cleartexts from the corresponding ciphertexts after a feasible computation.
So the algorithm of [1] is insecure.

1 Introduction

In [1] Matsumoto and Imai have developed a new public key scheme. The aim of this paper is to see how this scheme can be attacked.
For Crypto'95 this paper must be short. Also I have written an extended version of this paper which gives more proofs, details and examples than this short paper. I will be happy to give this extended version to anybody who wants it.

2 A short description of the Matsumoto-Imai Algorithm

2.1 A Mathematical Property

Let K be a finite field of characteristic 2, and let $q = 2^m$ be the number of elements of K (for example $K = GF(2)$ the field with 2 elements). Let L_N be an extension field of degree N of K, and let θ be an integer.

Then the function

$$f : \begin{array}{ccc} L_N & \rightarrow & L_N \\ x & \mapsto & x^{1+2^{m\theta}} \end{array}$$

is a bijection if $1 + 2^{m\theta}$ is coprime with $2^{mN} - 1$.
More precisely when f is a bijection f is easily invertible, and its inverse function f^{-1} is such that $f^{-1}(x) = x^{\hbar}$, where $\hbar$ is the multiplicative inverse of $1 + 2^{m\theta}$ modulo $2^{mN} - 1$.

D. Coppersmith (Ed.): Advances in Cryptology - CRYPTO '95, LNCS 963, pp. 248-261, 1995.

Let B be a basis of L_N, then the expression of f in the basis B is :

$$f(x_1, \ldots, x_N) = (p_1(x_1, \ldots, x_N), \ldots, p_N(x_1, \ldots, x_N))$$

where $p_1, \ldots, p_N$ are N polynomials in N variables of degree 2. The reason for this is that $x \mapsto x$ and $x \mapsto x^{2^{m\theta}}$ are both linear functions, so $f(x) = x.x^{2^{m\theta}}$ is a quadratic function and its components in the basis B have quadratic expressions.
The polynomials $p_1, \ldots, p_N$ are found by choosing a "representation" of L_N. Such a "representation" is typically given by the choice of an irreductible polynomial $i_N(X)$ over K, of degree N, so we can identify L_N with $K[X]/(i_N(X))$. It is then easy to find the polynomials $p_1, \ldots, p_N$.

2.2 Description of the Matsumoto-Imai Algorithm

The field K, with 2^m elements, is public. Each message will have $n.m$ bits, where n is another public integer.
n is split in $n = n_1 + \ldots + n_d$ with d integers $n_1, \ldots, n_d$. Then with these integers we will need d extensions of $K, L_{n_1}, \ldots, L_{n_d}$ of degree respectively $n_1, \ldots, n_d$. We will call "word" a value represented by some components of K. For example an element of L_{n_e}, $1 \leq e \leq d$, can be seen as a word of length n_e. Some quadratic functions $f_1, \ldots, f_d$ will be used, giving d words. These d words will then be recombined in a word of length n.

The secrets items will be :
1. Two affine bijections s and t from $K^n \rightarrow K^n$ (these affine bijections can be represented in a basis by polynomials of total degree 1 and with coefficients of the polynomials in K).
2. The separation of n in d integers : $n = n_1 + \ldots + n_d$.
3. The "representation" of the fields $L_{n_1}, \ldots, L_{n_d}$. These "representations" are given with the choice of d irreductible polynomials. We will denote by ψ_e the isomorphism from K^{n_e} to L_{n_e} given by these representations, $1 \leq e \leq d$.
4. Some integers $\theta_1, \ldots, \theta_d$ such that $1 \leq \theta_e < n_e$ and $GCD(2^{\theta_e} + 1, 2^{mn_e} - 1) = 1, 1 \leq e \leq d$. These integers θ_e give the quadratic functions $f_1, \ldots, f_d$ as we have seen in paragraph 2.1. (with $N = n_e$). (GCD is the Greatest Common Divisor function).

The enciphering is described in figure 1. (This figure must be read from the top to the bottom). The functions $\mu_1, \ldots, \mu_d$ are the function projections from K^n to K^{n_e}, and μ is the concatenation function.

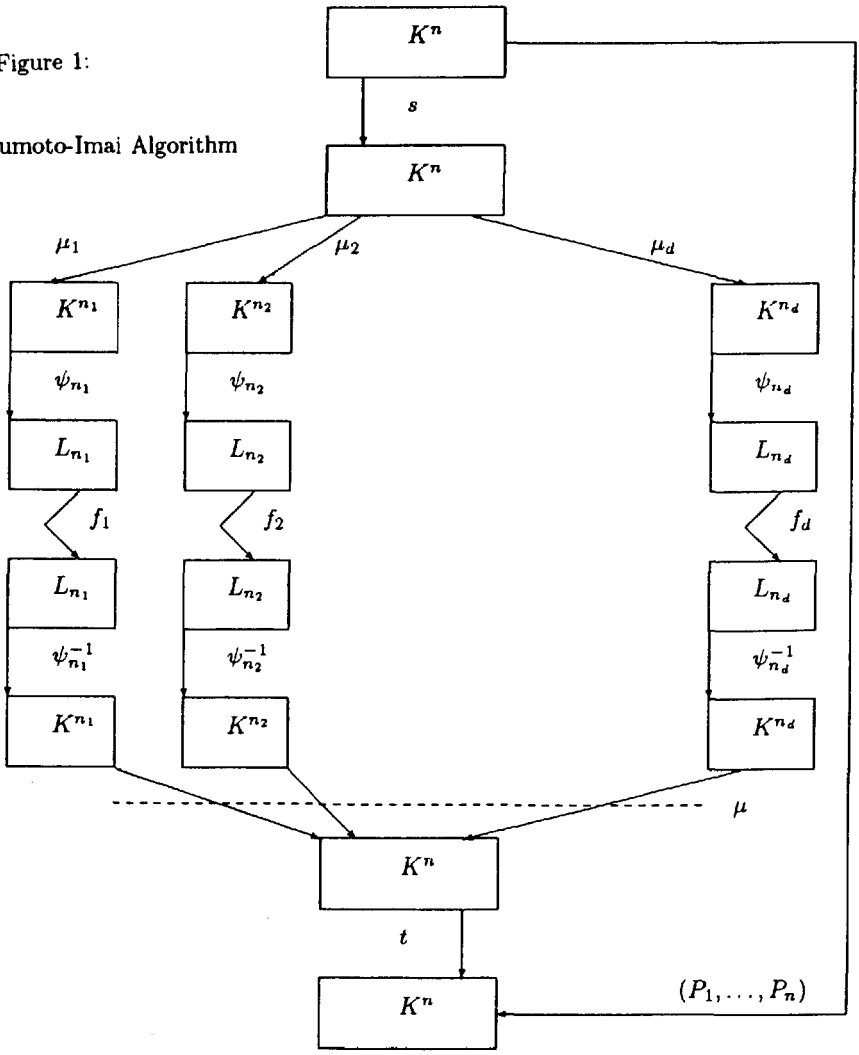
The important point is that the composition of all these operations is still a quadratic function in its components in a basis. So this function can be given by n polynomials over K, $(p_1, \ldots, p_n)$ (these polynomials give the ciphertext y from the cleartext x).

The public items are :
1. The field K of length 2^m, and the length n of the messages.
2. The n polynomials $(p_1, \ldots, p_n)$ in n variables over K.
So anyone can encipher a message.
Moreover to decipher is easy if the secret items are known : all the operations given in figure 1 will then be easily inverted. For example the quadratic functions f_e will be inverted by exponentiation $x \mapsto x^{h_e}$.

Note For various reasons (we explain these reasons in the extended version of this paper) Matsumoto and Imai limit themselves to the choice of integers θ_e and n_e such that there are some integers ℓ_e, r_e and b_e such that $n_e = (2\ell_e + 1).2^{r_e}$ and $\theta_e = b_e.2^{r_e}$, where $1 \leq b_e \leq \ell_e$.

Figure 1:

Matsumoto-Imai Algorithm



3 Complexity

The complexity of the public transformation is in $O(m^2n^3)$ and the complexity of the secret transformation is in $O((mn)^2(m+\log n))$, (cf.[1]).

Remark The m^2 coefficient in this expression comes from the fact that a multiplication of two elements of K requires $O(m^2)$ basic computations, and an addition of two elements of K requires $O(m)$ basic computations. However when m is not too big ($m \leq 8$ for example) we can store the table of the multiplication of two elements of K (and also the addition table if we want, but it is easy to compute addition in K without the table) and so computing the Matsumoto-Imai Algorithm will be about m^2 times quicker.

4 Our notations

Thoughout this paper (as in [1]), m is the degree of the field K chosen, n is the number of components of K that we have in each message, and d is the number of integers in the secret split of n : $n = n_1 + \ldots + n_d$.
Let e be an index, $1 \leq e \leq d$, and let x be the plaintext and y the ciphertext. In this paper we will also denote by L_{n_e} the extension field of degree n_e over K, by a_e the element of L_{n_e} affine in x, by b_e the element of L_{n_e} affine in y, and by θ_e the secret parameter such that $b_e = a_e^{1+2^{m\theta_e}}$. (So, with the notations of Figure 1 that we will not use any more, we have $a_e = \psi_{n_e}(\mu_e(s(x)))$). Moreover in order to simplify the notations throughout this paper we will denote most of the time θ_e by θ, a_e by a, and b_e by b.
Figure 1 becomes Figure 2 with these notations :

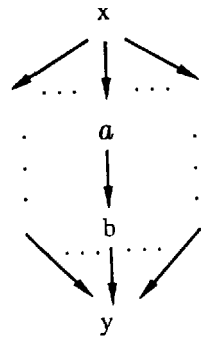


Figure 2: Our notations for the Matsumoto-Imai Algorithm. $b = a^{1+2^{m\theta_e}}$ is quadratic in a, a is affine in x and b is affine in y.

5 A family of weak keys

In this paragraph we will show that there are some weak keys in the Matsumoto-Imai algorithm. It does not seem that Matsumoto and Imai where aware of these

weak choices. However it is very easy to avoid these weak keys, so it's not a very serious problem for the Matsumoto-Imai Algorithm. (In the following paragraphs we will see much more serious problems).

Let us again use the notations of paragraph 4, with x the plaintext, y the ciphertext, a affine in x, b affine in y, and $b = a^{1+2^{m\theta_e}}$ (1) (in a field L_{n_e} of degree n_e over K).

The equation (1) can also be written : $a = b^{\hbar_e}$, where $\hbar_e$ is the inverse multiplicative of $(1 + 2^{m\theta_e})$ modulo $2^{mn_e} - 1$.
If α is an integer, let us denote by $HW(\alpha)$ the number of 1 in the expression of α in base 2. (HW stands for "Hamming Weight in base 2").
Let x_i be the bits of x and y_i be the bits of y, $1 \leq i \leq mn$.
Each value $y_j, 1 \leq j \leq n$, has a quadratic expression in the values $x_i, 1 \leq i \leq n$. Similary each value x_j has an expression as a polynomial of degree $\sup_{e,1\leq e\leq d} HW(\hbar_e)$ in the values y_i. So, in order to make this expression of the $x_j, 1 \leq j \leq n$, as polynomials in the $y_i, 1 \leq i \leq n$, impractible, it is necessary for **at least one** variable e, that $HW(\hbar_e)$ be not too small (for example $HW(\hbar_e) \geq 6$ for **at least one** variable e). This fact was very clear from [1], but we will see now that in fact it is much better if for **all** variables e $HW(\hbar_e)$ is not too small (for example $HW(\hbar_e) \geq 6$ for **all** variables e).

Let us assume that this is not the case, i.e. that for one variable $e, 1 \leq e \leq d$, $HW(\hbar_e)$ is very small and : $a = b^{\hbar_e}$ (2).
Let a_i be the bits of a and b_i be bits of b in a basis, $1 \leq i \leq n_e m$.
Since a is affine in x, there are some values $\alpha_{1i}, 0 \leq i \leq nm$, such that $a_1 = \alpha_{10} + \sum_{i=1}^{nm} \alpha_{1i} x_i$.
From (2) we know that a_1 has a polynomial expression of total degree $HW(\hbar_e)$ in $b_1, \ldots, b_{n_e m}$. Since all these values $b_1, \ldots, b_{n_e m}$ are affine in $y_1, \ldots, y_{nm}$, a_1 has a polynomial expression of total degree $HW(\hbar_e)$ in $y_1, \ldots, y_{nm}$.
So there is a polynomial P of total degree $HW(\hbar_e)$ such that :

$$\alpha_{10} + \sum_{i=1}^{nm} \alpha_{1i} x_i = P(y_1, \ldots, y_{nm}) \quad (3).$$

And it's the same for $a_2, a_3, \ldots, a_{n_e m}$. So there is at least $n_e m$ equations similar to (3), of degree 1 in the x_i, and of total degree $HW(\hbar_e)$ in the y_i. So if for a particular e, $HW(\hbar_e)$ is very small, (say $HW(\hbar_e) \leq 4$ for example) we will be able to find these $n_e m$ equations similar to (3) (and this even if there is another index f such that $HW(\hbar_f)$ is very big). In order to find these equations, we will simply write the most general form of such an equation of degree $HW(\hbar_e)$, and by generating some values for x and y from the public form, we will obtain some equations of degree 1 in the coefficients of the polynomials.
After collecting sufficiently such equations by Gaussian reduction on these equa-

tions we will find the vectorial space of solution for the coefficients of the polynomials. So we will find at least $n_e m$ independent equations similar to (3).

Now from these equations, when y is given, we have immediatly $n_e m$ equations of degree one on the bits x_i of the cleartext. This may be a very dangerous thing in some applications, and at least it allows the cryptanalyst to do the exhaustive search in $2^{(n-n_e)m}$ instead of 2^{nm} on the cleartext.

Conclusion : All the values n_e and θ_e must be chosen in order that $HW(\hbar_e)$ is not too small (say ≥ 6 for example).

6 Our first general attack on all the keys

6.1 An example

Let us use again the notations of paragraph 4, with x the plaintext, y the ciphertext, a affine in x, b affine in y, and $b = a^{1+2^{m\theta}}$. (We are looking at what happening in $L_{n_e}, 1 \leq e \leq d$).
In this example, we will assume that $m = 1$ and $\theta = 1$ (the general case will be considered in paragraph 6.2). So

$$b = a^3. \quad (1).$$

Let $(b_1, \ldots, b_{n_e})$ be the representation of b in L_{n_e}, and let $(a_1, \ldots, a_{n_e})$ be the representation of a in L_{n_e}.
From (1) we see that all the $b_j, 1 \leq j \leq n_e$, have a quadratic expression in $(a_1, \ldots, a_{n_e})$, because $b = a.a^2$, and a^2 is linear (because here $m = 1$).
However we would like to find a useful expression which gives the a_j values from the b_j values (instead of the b_j values from a_j values).
The first idea is of course to write

$$a = b^{\hbar} \quad (2),$$

but in most cases $HW(\hbar)$ is big so (2) gives an intractable expression for the a_j values. So, what should be done ?
Let us start again from (1) and multiply both terms of (1) by a.
We obtain :

$$b.a = a^4. \quad (3).$$

The equation (3) gives n_e equations of degree one on the b_j values **and** of degree one on the a_j values !! (because a^4 is linear in a, because $m = 1$ here).

Moreover for any $b \neq 0$, there are exactly two solutions of (3) : the solution $a = 0$, and the solution $a = b^{\hbar}$. So in a way with (3) we will loose one equation over $GF(2)$, but the important point is that this equation (3) will be useful even if the equation (2) is intractable.

a is affine in x, b is affine in y, and a^4 is linear in a.
So from equation (3), we know that there are some equations of the form :

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\gamma_{ij}x_iy_j + \sum_{i=1}^{n}\alpha_i x_i + \sum_{i=1}^{n}\beta_i y_i + \delta_0 = 0. \quad (4)$$

These equations are true for all the x, y, when x is the plaintext of y. Moreover if $b = 0$, there is only one solution for a of (3). So we must necessary have at least n_e "formally" independent equations like (4). ("Formally" means here that the vectorial space of the solutions for the values $\gamma_{ij}, \alpha_i, \beta_i$ and δ_0 is at least n_e). However, for a given value y we can just say that we will have at least $n_e - 1$ independent equations (4) (and not n_e) because (3) has two solutions in a when $b \neq 0$.

By choosing some values for x and computing the value y from x and the public form, and then by replacing these values x_i and $y_i, 1 \leq i \leq n$ in (4), we will obtain some equations of degree one in the $n^2 + n + n + 1 = (n+1)^2$ variables $\gamma_{ij}, \alpha_i, \beta_i$ and δ_0.
In this way we are able to find quickly all the equations (4) (by Gaussian reductions). Then, from a given y for which we want to find x, these equations give us some equations (at least $n_e - 1$ independent equations) of degree one on the values $x_1, \ldots, x_n$. So by Gaussian reduction, we are able to find $n_e - 1$ variables $x_1, \ldots, x_m$ from the others.
Let us now see the general case.

6.2 The general case

Let us again use the notations of paragraph 4. We have

$$b = a^{1+2^{m\theta}}. \quad (5).$$

By composition on each side of this equation with $g : x \mapsto x^{2^{m\theta}-1}$, we obtain :

$$b^{2^{m\theta}-1} = a^{2^{2m\theta}-1}.$$

Now let us multiply each side by $a.b$. We obtain :

$$a.b^{2^{m\theta}} = b.a^{2^{2m\theta}}. \quad (6).$$

Let $(a_1, \ldots, a_{n_e})$ be the representation of a in L_{n_e}, and $(b_1, \ldots, b_{n_e})$ be the representation of b in L_{n_e}. (So all the a_i and b_i, $1 \leq i \leq n_e$, are elements of K).
This equation (6) gives n_e equations (not necessarily independent) of degree one on the b_j values **and** of degree one on the a_j values ! (because $b \mapsto b^{2^{m\theta}}$ is linear, and $a \mapsto a^{2^{2m\theta}}$ is linear, i.e. in a basis the n_e components of $b^{2^{m\theta}}$ can be written as a polynomial of degree one in the components of b, with coefficients of the polynomial in $K = GF(2^m)$).

Moreover a is affine in x, and b is affine in y. So these n_e equations ((6) in a basis) when we write them in the components $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ of x and y give n_e equations of the form :

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\gamma_{ij}x_iy_j + \sum_{i=1}^{n}\alpha_i x_i + \sum_{i=1}^{n}\beta_i y_i + \delta_0 = 0. \quad (7).$$

These equations are true for all x, y when x is the plaintext of y. So by choosing some values for x and computing the value y from x and the public form, and then by replacing these values x_i and $y_i, 1 \leq i \leq n$, in (7), we will obtain some equations of degree one in the $(n+1)^2$ variables of $GF(2^m)$: $\gamma_{ij}, \alpha_i, \beta_i$ and δ_0.

By this way we are able to find quickly, by Gaussian reductions, all the equations (7). This is the Part 1 of our Attack. Maybe we will find some equations (7) which do not come from the equation (6) (because we found all the equations which have the general form of (7)), but the important point is that at least we will found all the equations (7) which come from (6).
Part 2 of our attack : then, from a given y for which we want to find x, these equations will give us some equations of degree one on the values $x_1, \ldots, x_n$. By Gaussian reduction these equations will allow us to find λ variables $x_1, \ldots, x_n$ from the others, where λ is the number of independent equations (7) in $x_1, \ldots, x_n$ when $y_1, \ldots, y_n$ are replaced by the value we want. So, in order to evaluate the power of this attack, we have to evaluate λ. This is what we will do now.

Remark If $m = 1$ and $\theta_e = 1$ (and whatever the value of n_e) when we will find all the equations (7) we will find all the equations which come from $b^2.a = b.a^4$ **and** all the equations which come from $b.a = a^4$, and these equations are not formally the same (because if $b = 0$ the first ones vanish, but not the second ones). For example, when $m = 1$, $\theta = 1$, and $n_e = 5$ we have explicitely found all the equations (7). In this case we have found a vectorial space of solutions for the coefficients $\gamma_{ij}, \alpha_i, \beta_i$ and δ_0 of dimension exactly 10. In that case $b^2.a = b.a^4$ and $b.a = a^4$ gives 10 equations. When we choose for y a given value, these 10 equations will of course give us at most 5 independent equations, and if for this y we have $b \neq 0$, when they will give us exactly 4 independent equations (because we have exactly two solutions for a).

6.3 Evaluation of λ

Theorem 6.3 *For all the practical keys and for most of the ciphertexts y, the number λ of independent equations of degree one in $x_1, \ldots, x_n$ that we will obtain from the equations (7) for this given y is $\lambda \geq \sum_{e=1}^{d}(n_e - GCD(\theta_e, n_e)) \geq \frac{2n}{3}$. Moreover this shows that for a lot of secret keys for most of ciphertext we will have $\lambda \geq n - d$.*

For the proof of this Theorem, we will need three lemmas.

Lemma 1 *Let L be a finite field with q elements. Let p be an integer, and let y be an element of L. Then the equation $x^p = y$ has at most $GCD(p, q-1)$ solutions x.*

Proof of Lemma 1

If $y = 0$, then $x = 0$ is the only solution, and a lemma 1 is true.
So we can assume that $y \neq 0$. Then $x = 0$ is not solution, so we can assume also that $x \neq 0$, so $x^{q-1} = 1$.
Let $\mu = GCD(p, q-1)$.
From Bezout Theorem we know that there are two integers α and β such that $\alpha p - \beta(q-1) = \mu$. So

$$\begin{aligned} x^p = y &\Rightarrow x^{\alpha p} = y^{\alpha} \\ &\Rightarrow x^{\mu}.(x^{q-1})^{\beta} = y^{\alpha} \\ &\Rightarrow x^{\mu} = y^{\alpha}. \end{aligned}$$

In a field (commutative by definition) each equation of degree k has at most k solutions. So there is at most μ solutions of $x^{\mu} = y^{\alpha}$, and so there is at most μ solutions of $x^p = y$, as claimed.

Lemma 2 *For all integers m, α and β we have :*

$$GCD(2^{m\alpha} - 1, 2^{m\beta} - 1) = 2^{mGCD(\alpha,\beta)} - 1.$$

Proof of lemma 2

- Clearly $GCD(2^{m\alpha} - 1, 2^{m\beta} - 1) \geq 2^{mGCD(\alpha,\beta)} - 1$, because in $2^{m\alpha} - 1$ and $2^{m\beta} - 1$ we can put $2^{mGCD(\alpha,\beta)} - 1$ in factor (use the formula $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \ldots + x + 1)$).
- Clearly also, we can assume that $\alpha > \beta$ by the symmetry of the hypothesis in lemma 2 and since when $\alpha = \beta$ lemma 2 is obvious.
- Now if x and y are two integers, and if μ is an integer such that $x - y.2^{\mu} > 0$, we have :

$$GCD(x, y) = GCD(y, x - y.2^{\mu}).$$

So with $x = 2^{m\alpha} - 1, y = 2^{m\beta} - 1$ and $2^{\mu} = 2^{m(\alpha-\beta)}$ we have :

$$GCD(2^{m\alpha} - 1, 2^{m\beta} - 1) = GCD(2^{m\beta} - 1, 2^{m(\alpha-\beta)} - 1). \quad (8).$$

By iterating this technique, $GCD(\alpha, \beta)$ will appear in a way similar to the computation of $GCD(\alpha, \beta)$ by the euclidian algorithm so we will obtain:$GCD(2^{m\alpha} - 1, 2^{m\beta} - 1) \leq 2^{mGCD(\alpha,\beta)} - 1$.

Lemma 3 *In L_{n_e} (the field with 2^{mn_e} elements) the equation (6) that we have written before :*
$a.b^{2^{m\theta}} = b.a^{2^{2m\theta}}$ *(6), has at most $2^{mGCD(\theta,n_e)}$ solutions in a, for each given $b \neq 0$.*

Proof of lemma 3

When $b \neq 0$ this equation (6) has two families of solution a :
1) $a = 0$.
2) a such that : $(a^{2^{m\theta}-1})^{2^{m\theta}+1} = b^{2^{m\theta}-1}$. (9).

We know that the function $g : z \mapsto z^{2^{m\theta}+1}$ is a bijection in L_{n_e} (because by construction of the Matsumoto-Imai Algorithm θ and n_e are chosen in order to have this property).
So a is solution of (9) if and only if :

$$a^{2^{m\theta}-1} = g^{-1}(b^{2^{m\theta}-1}). \quad (10).$$

Now from lemma 1 we know that this equation (10), for a given b has at most $GCD(2^{m\theta}-1, 2^{mn_e}-1)$ solutions a.
So with lemma 2 we obtain that (9) has at most $2^{mGCD(\theta,n_e)}-1$ solutions in a.
So, by adding the solution $a = 0$, we obtain that : when $b \neq 0$, (6) has at most $2^{mGCD(\theta,n_e)}$ solutions in a, as claimed.

Corollary of lemma 3

For a given $b \neq 0$, if we write the equation (6) in a basis on the components of a (i.e. with a representation of L_{n_e} as an extension of degree n_e of $GF(2^m)$), then we will obtain at least $n_e - GCD(\theta, n_e)$ independent equations of degree one in the components of a.

Proof of the corollary

We have seen that the equations that we obtain are of degree one in the components of a. Moreover these equations have at least one solution : $a = 0$, so there is no contradiction in these equations. If λ_e is the number of independent equations, we will have exactly $2^{m(n_e-\lambda_e)}$ solutions. However from Lemma 3 we know that we have at most $2^{mGCD(\theta,n_e)}$ solutions. So $\lambda_e \geq n_e - GCD(\theta, n_e)$, as claimed.

Proof of theorem 6.3

(Here exceptionally we will use the notations a_e, b_e, and θ_e for a, b and θ because we will need the d values e, $1 \leq e \leq d$).
Let y be a ciphertext such that for this y we have :
$\forall e, 1 \leq e \leq d, b_e \neq 0$. (So $a_e \neq 0$ as well, since $b_e = a_e^{1+2^{m\theta_e}}$).

Note. For a given e, the probability that $b_e = 0$ is $1/2^{mn_e}$. So if mn_e is very small this probability may not be negligible. However if mn_e is very small (for example if $m = 1$ and $n_e = 3$) then $a_e = b_e^{\hbar_e}$ with a very small $\hbar_e$, so with a very small $HW(\hbar_e)$, and we have seen in paragraph 5 that this gives very weak keys. (We have seen that in this case it is easy to "eliminate" the variables of the branch number e).

So we can assume that mn_e is not so small, and so that "most" of the ciphertexts y will be such that $\forall e, 1 \leq e \leq d, b_e \neq 0$. (For very big d this may not be the case, but if n is of a reasonable size, then d cannot be too big and for most ciphertext y, $\forall e, 1 \leq e \leq d$, $b_e \neq 0$ as claimed).

We have seen in paragraph 6.2 that in the equations (7) we will find at least all the equations which come from all the equations (6) when we write these equations with the components of x and y instead of a and b, and this for all the values of $e, 1 \leq e \leq d$.

So from the Corollary of Lemma 3, we know that we will obtain at least $\sum_{e=1}^{d}(n_e - GCD(\theta_e, n_e))$ independent equations of degree one in the components of x (for each given y such that $\forall e, b_e \neq 0$).
So we have proved the first part of Theorem 6.3.

We will now need another lemma.

Lemma 4 *$\forall e, 1 \leq e \leq d$, let $\delta_e = GCD(\theta_e, n_e)$, and let $k_e = n_e/\delta_e$ (k_e is an integer because δ_e divides n_e). Then k_e is always odd, and $k_e \geq 3$.*

Proof of lemma 4

We know from the values chosen in [1] that we can write $n_e = \alpha.2^r$ and $\theta_e = \beta.2^s$ with α and β odd and $s \geq r$. (This is also explain in the extended version of this paper).
So $\delta_e = 2^r GCD(\alpha, \beta)$, and $k_e = \alpha/GCD(\alpha, \beta)$, with α and β odd.
So k_e is odd. Moreover $\theta_e < n_e$, so $\delta_e < n_e$, so $k_e > 1$, so $k_e \geq 3$.

We can now finish the proof of Theorem 6.3.
We have proved that $\lambda \geq \sum_{e=1}^{d}(n_e - GCD(\theta_e, n_e))$.
So from Lemma 4, $\lambda \geq \sum_{e=1}^{d}(n_e - \frac{n_e}{3}) = \frac{2}{3}\sum_{e=1}^{d} n_e = \frac{2n}{3}$.
Moreover for a lot of secret keys $GCD(\theta_e, n_e) = 1$, and if that occurs we have $\sum_{e=1}^{d}(n_e - 1) = n - d$, so $\lambda \geq n - d$.

6.4 Improved Gaussian elimination

Our attack, as we have described it, proceeds in two parts :

Part 1. We find all the equations (7), and this has to be done once and for all.

Part 2. For a specific ciphertext y, we try to find x with the help of equations (7). So this has to be done each time we have another x to find from another y.

In Part 1 we have to do a Gaussian reduction on $(n+1)^2$ variables and about $(n+1)^2$ equations of $GF(2^m)$. So in the most general case our Part 1 will have a complexity of at most $m^2.n^6$.
In most practical cases Part 1 will be dominant in time from Part 2. So it is worth improving Part 1. This is what we do in the extended version of this paper where we show that there is an Algorithm in $O(m^2n^4 \log n)$ for Part 1 instead $O(m^2n^6)$. (The idea is to choose some values of x in order to have a more easy Gaussian reduction).

7 Our second general attack

7.1 Description of the second attack

In paragraph 6 our attack was based on the idea that if $b = a^{1+2^{m\theta}}$, then $a.b^{2^{m\theta}} = b.a^{2^{2m\theta}}$ (6).
In equation (6) a and b are on both sides.
In this paragraph 7 we will now try to find some equations of the general form :

$$a^2.b^u = b^v$$

with $HW(u)$small and $HW(v)$ small. (Here a is only on one side of the equation).

For this purpose we will not start from $b = a^{1+2^{m\theta}}$, but we will start from $a = b^{\hbar_e}$. So we will have to evaluate the value of $\hbar_e$.

Theorem 7.1 *Let $\delta = mGCD(\theta_e, n_e)$, and let α and k be integers such that $\alpha\delta = m\theta_e$, and $k\delta = mn_e$. Let $\hbar_e$ be, as usual, the multiplicative inverse of $1 + 2^{m\theta_e}$ modulo $2^{mn_e} - 1$.*
Then : **1.** *k is odd and $k \geq 3$.*
and : **2.** $\hbar_e = 2^{k\delta-1} + \sum_{i=1}^{k-1}(-1)^i.2^{\alpha\delta i-1}$.

Proof

$k = n_e/GCD(\theta_e, n_e)$ and from Lemma 4 of paragraph 6 we know that this value is odd and ≥ 3. So k is odd and $k \geq 3$.
Now $1 - 2^{\alpha\delta} + 2^{2\alpha\delta} + \ldots + (-2^{\alpha\delta})^{(k-1)} = (1 - (-2^{\alpha\delta})^k)/(1 + 2^{\alpha\delta})$.
(Because this is a well know sum of a geometric series).

So we have :

$$(1 + 2^{\alpha\delta})\left(1 + \sum_{i=1}^{k-1}(-1)^i.2^{\alpha\delta i}\right) = 1 - (-1)^k(2^{k\delta})^\alpha.$$

So since k is odd, we have :

$$(1+2^{\alpha\delta})\left(2^{k\delta}+\sum_{i=1}^{k-1}(-1)^i.2^{\alpha\delta i}\right)=2 \quad \text{modulo} \quad (2^{k\delta}-1).$$

So $2^{k\delta-1}+\sum_{i=1}^{k-1}(-1)^i.2^{\alpha\delta i-1}$ is the multiplicative inverse of $1+2^{m\theta_e}$ modulo $2^{mn_e}-1$, as claimed.

From $a^2=b^{2\hbar_e}$ and Theorem 7.1 we have :

$$a^2.b^u=b^v, \quad \text{with } u=\sum_{i=1}^{(k-1)/2}2^{m\theta_e(2i-1)} \text{ and } v=1+\sum_{i=1}^{(k-1)/2}2^{2m\theta_e i}.$$

So $HW_m(u)=(k-1)/2$ and $HW_m(v)=(k+1)/2$, where $HW_m(z)$ denotes the minimum number of terms when we write z as powers of 2^m.
So the equation $a^2.b^u=b^v$, when we write it as n_e equations in the components x_i^2 and y_i gives n_e equations of degree one in the x_i^2, and of total degree $(k+1)/2$ in the y_i.

Remark In paragraph 6 the most difficult keys were the keys with very small k. Strangely theses keys are the easiest keys in this paragraph 7.

For example when $k=3$ we will obtain n_e equations of the general form :

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\gamma_{ij}x_i^2y_j+\sum_{i=1}^{n}\sum_{j=i+1}^{n}\eta_{ij}y_iy_j+\sum_{i=1}^{n}\alpha_ix_i+\sum_{i=1}^{n}\beta_iy_i+\delta_0=0 \quad (9).$$

Our attack will then still be in two Parts.

Part 1. We will find all the equations (7) of paragraph 6 and also all the equations (9) (as usual by Gaussian reduction after computing some couples (x,y) from the public form).

Part 2. Then for a given y we will put to the power 2^{m-1} the equations (9) found. Since in K we have $(\alpha+\beta)^{2^{m-1}}=\alpha^{2^{m-1}}+\beta^{2^{m-1}}$ and since $x_i^{2^m}=x_i$, the equations (9) will give us like this equations of degree one in the x_i. Therefore we will use both equations (7) and (9).

Note 1. Here, when $k=3$, the Gaussian reduction for Part 1 is in m^2n^6 (instead of $m^2n^4\log n$), so Part 1 takes more time with this attack. However Part 2 will be quicker because for all $b\neq 0$, there is only one solution in a to $a^2.b^u=b^v$. Since Part 1 has to be done only once we see that $k=3$ is not a good choice.

Note 2. Another solution would have been to write all the equations (9) on the bits. However the complexity for Part 1 when $k = 3$ would then have been in $O(m^6 n^6)$ instead of $O(m^2 n^6)$.

7.2 An example of attack

In [1] p. 435 we know that an implementation with $m = 8$ and $n = 32$ has been done. We know nothing about the secret keys chosen. Whatever the value of the secret key we will be able to find a cleartext from a ciphertext of this implementation after at most 2^{32} computations, and much less most of the time, with our attacks of paragraph 6 and 7. (More details are given about this example in the extended version of this paper).

8 Further Improvements

If for some index e, mn_e is not too big (for example if $mn_e \leq 32$), then we have found that it is possible to further improve our attacks. We will do more computations to be done once and for all but less to be done for each message. We have no room here to explain these improvements in details but the idea is to use the fact that for some values of the x_i the number of independent equations (7) in the y_i decreases suddenly. This comes from the fact that when $a = 0$ our equations (6) of paragraph 6 becomes $0 = 0$. So these values of the x_i give useful information that allow us when mn_e is not too big to "separate" the variables. (More details are given about this in the extended version of this paper).

9 Conclusion

In this paper we have seen that the scheme of [1] is insecure. Whatever the value of the keys we are able to find easily most of the cleartexts from their ciphertexts, at least for texts of reasonable size. Some different schemes based on similar ideas may be much more difficult to break. However the choice of the secret keys and the choice of these variations will have to be done with great care.

Acknowledgements

I want to thank Paul Camion, Daniel Augot and Sandrine Grellier for their descriptions of the Matsumoto-Imai Algorithm.

References

[1] T. Matsumoto and H. Imai, *Public Quadratic Polynomial-tuples for efficient signature-verification and message-encryption*, EUROCRYP'88, Springer-Verlag 1988, pp. 419-453.