Cryptanalysis of the TTM Cryptosystem

Louis Goubin and Nicolas Courtois

Bull CP8
68 route de Versailles – BP45
78431 Louveciennes Cedex
France
Louis.Goubin@bull.net,courtois@minrank.org

Abstract. In 1985 H. Fell and W. Diffie studied a paradigm for constructing public key cryptosystems based on sequentially solved multivariate equations [9], which can be seen as a triangular system. In the present paper, we study a more general family of TPM (for "Triangle Plus Minus") schemes. A TPM is a triangular construction, with added u final random polynomials and r beginning equations removed.

We go beyond all previous attacks proposed on such cryptosystems, that used the low degree of a component of the inverse function. We show that the the cryptanalysis of TPM reduces to solving a simple linear algebra problem called *MinRank(r)*: Find a linear combination of given matrices that has a small rank r.

We present a new algorithm for the MinRank(r) problem and the TPM cryptosystems. It is called 'Kernel Attack' and is polynomial for a fixed r. As an application of this technique, we present two different attacks on the TTM cryptosystem proposed by T.T. Moh at CrypTec'99 [13, 14] with $r = 2$.

Though the TTM cleartext is 512 bits long, we are able to completely break TTM (*i.e.* to recover the secret key) in $\mathcal{O}(2^{52})$. Moreover, the particular cryptosystem described in [13, 14] has additional weaknesses that allows an attack in $\mathcal{O}(2^{28})$.

The attacks we describe are both theoretical and pratical: as an example, we present the solution to the TTM 2.1 challenge proposed by the company US Data Security, currently selling implementations of TTM. We conclude that no scheme in the TPM class is secure.

1 Introduction

The research effort to bring further the practical public key cryptography introduced by R. Rivest, A. Shamir and L. Adleman, with univariate polynomials over $\mathbf{Z}/N\mathbf{Z}$, is following two paths. The first is considering more complex groups, e.g. elliptic curves. The second is considering multivariate equations. Many proposed schemes are being broken, some of them remain unbroken even for the simplest groups like $\mathbf{Z}/2\mathbf{Z}$.

One of the paradigms for constructing multivariate trapdoor cryptosystems is the triangular construction, proposed initially in an iterated form by H. Fell and W. Diffie (1985). It uses equations that involve 1, 2, ..., n variables and are solved sequentially. The special form of the equations is hidden by two linear transformations on inputs (variables) and outputs (equations). We call T this triangular construction. Let TPM (T Plus-Minus) be T with added final random polynomials and with some of the beginning equations removed.

The cryptosystem TTM has been proposed by T.T. Moh at CrypTec'99. TTM, in spite of apparent complexity, proved to be a subcase of TPM design. After showing a trivial attack using linearities of initially proposed TTM, we focus on breaking more general TPM schemes.

Recovering the secret key of TPM/TTM leads to the following linear algebra problem called MinRank. Let M be a $n \times n$ matrix with entries being linear combinations of variables $\lambda_1, \ldots, \lambda_t$ over GF(q). The MinRank problem consists in determining whether there is such a valuation for $\lambda_1, \ldots, \lambda_t$ that Rank(M) $\leq r$. The weakness of MinRank instances in TTM lies in the fact that r is small ($r = 2$ in T.T. Moh's paper), while in general MinRank is NP-complete.

First we present an attack that works when q^r is small, exploiting the small co-dimension of the kernel of the unknown matrix. Our attacks break in approximately 2^{52} a cryptosystem with 512 bit cleartexts. In section 6, we present the solution (plaintext) to the TTM 2.1 challenge proposed by the company US Data Security, which is currently selling implementations of TTM. Finally, in section 5, we present an attack that works on TPM signature schemes when q^u is not too large and breaks TTM signature proposals [13, 14]. As a result, we conclude that no scheme in the TPM class is secure.

2 The TPM Family of Cryptosystems

2.1 General Description of TPM

In the present section, we describe the general family TPM(n, u, r, K), with:

- n, u, r integers such that $r \leq n$. We also systematically put $m = n + u - r$.
- $K =$ GF(q) a finite field.

We first consider a function $\Psi : K^n \mapsto K^{n+u-r}$ such that $(y_1, \ldots, y_{n+u-r}) = \Psi(x_1, \ldots, x_n)$ is defined by the following system of equations:

$$\begin{cases} y_1 = x_1 + g_1(x_{n-r+1}, \ldots, x_n) \\ y_2 = x_2 + g_2(x_1 \; ; x_{n-r+1}, \ldots, x_n) \\ y_3 = x_3 + g_3(x_1, x_2 \; ; x_{n-r+1}, \ldots, x_n) \\ \quad \vdots \\ y_{n-r} = x_{n-r} + g_{n-r}(x_1, \ldots, x_{n-r-1} \; ; x_{n-r+1}, \ldots, x_n) \\ y_{n-r+1} = g_{n-r+1}(x_1, \ldots, x_n) \\ \quad \vdots \\ y_{n-r+u} = g_{n-r+u}(x_1, \ldots, x_n) \end{cases}$$

with each g_i ($1 \leq i \leq n + u - r$) being a randomly chosen quadratic polynomial.

The Public Key

The user selects a random invertible affine transformation $s: K^n \mapsto K^n$, and a random invertible affine transformation $t: K^{n+u-r} \mapsto K^{n+u-r}$. Let $F = t \circ \Psi \circ s$. By construction, if we denote $(y'_1, \ldots, y'_{n+u-r}) = F(x'_1, \ldots, x'_n)$, we obtain an explicit set $\{P_1, \ldots, P_{n+u-r}\}$ of $(n+u-r)$ quadratic polynomials in n variables, such that:

$$\begin{cases} y'_1 = P_1(x'_1, \ldots, x'_n) \\ \quad \vdots \\ y'_{n+u-r} = P_{n+u-r}(x'_1, \ldots, x'_n) \end{cases}$$

This set of $(n+u-r)$ quadratic polynomials constitute the public key of this TPM(n, u, r, K) cryptosystem. Its size is $\frac{1}{8}(n+u-r)(n+1)(\frac{n}{2}+1)\log_2(q)$ bytes.

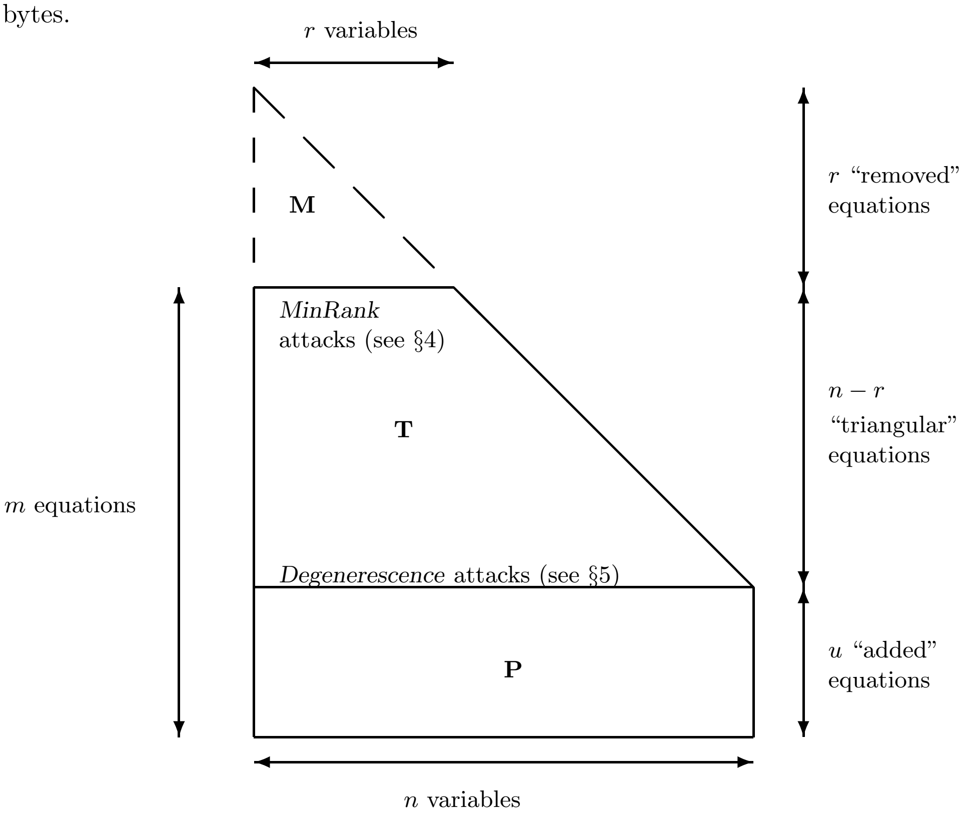
r variables
M
r "removed" equations
MinRank attacks (see §4)
T
$n - r$ "triangular" equations
m equations
Degenerescence attacks (see §5)
P
u "added" equations
n variables

Fig. 1. General view of the TPM scheme – The two classes of attacks

2.2 Encryption Protocol (when $u \geq r$)

Encrypting a message

Given a plaintext $(x'_1, \ldots, x'_n) \in K^n$, the sender computes $y'_i = P_i(x'_1, \ldots, x'_n)$ for $1 \leq i \leq n+u-r$ – thanks to the public key – and sends the ciphertext $(y'_1, \ldots, y'_{n+u-r}) \in K^{n+u-r}$.

Decrypting a message
Given a ciphertext $(y'_1, \dots, y'_{n+u-r}) \in K^{n+u-r}$, the legitimate receiver recovers the plaintext by the following method.

- Compute $(y_1, \dots, y_{n+u-r}) = t^{-1}(y'_1, \dots, y'_{n+u-r})$;
- Make an exhaustive search on the r-tuple $(x_{n-r+1}, \dots, x_n) \in K^r$, until the n-tuple $(x_1, \dots, x_n)$ obtained by $x_i = y_i - g_i(x_1, \dots, x_{i-1}; x_{n-r+1}, \dots, x_n)$ (for $1 \leq i \leq n-r$) satisfies the u following equations $g_i(x_1, \dots, x_n) = y_i$ (for $n-r+1 \leq i \leq n-r+u$).
- For the obtained $(x_1, \dots, x_n)$ n-tuple, get $(x'_1, \dots, x'_n) = s^{-1}(x_1, \dots, x_n)$.

This decryption algorithm thus has a complexity essentially $\mathcal{O}(q^r)$. As a result, a TPM(n, u, r, K) cryptosystem can be practically used in encryption mode only under the assumption that q^r is "small enough".

The condition $u \geq r$ insures that the probability of obtaining a collision is negligible, and thus that the ciphering function F can be viewed as an injection from K^n into K^{n+u-r}.

When $r = u = 0$, this kind of scheme was already considered and attacked by H. Fell and W. Diffie in [9] (in an iterated form) and by J. Patarin and the first author in [16]. All these authors heavily use the fact that the inverse function if of low degree on some of its variables. The goal of this paper is to extend these attacks to a much more general case, with r being non-zero (but q^r is not too large) and u is non-zero.

2.3 Signature Protocol (when $u \leq r$)

Signing a message
Given a message M, we suppose that $(y'_1, \dots, y'_{n+u-r}) = h(M) \in K^{n+u-r}$, with h being a (collision-free) hash function. To sign the message M, the legitimate user:

- computes $(y_1, \dots, y_{n+u-r}) = t^{-1}(y'_1, \dots, y'_{n+u-r})$;
- chooses random r-tuples $(x_{n-r+1}, \dots, x_n)$, until the n-tuple $(x_1, \dots, x_n)$ obtained by $x_i = y_i - g_i(x_1, \dots, x_{i-1}; x_{n-r+1}, \dots, x_n)$ (for $1 \leq i \leq n-r$) satisfies the u following equations $g_i(x_1, \dots, x_n) = y_i$ (for $n-r+1 \leq i \leq n-r+u$).
- for the obtained $(x_1, \dots, x_n)$ n-tuple, gets $(x'_1, \dots, x'_n) = s^{-1}(x_1, \dots, x_n)$.

This signature algorithm thus has a complexity essentially $\mathcal{O}(q^u)$. As a result, a TPM(n, u, r, K) cryptosystem can be practically used in signature mode only under the assumption that q^u is "small enough".

The condition $u \leq r$ insures that the probability of finding no solution for $(x_1, \dots, x_n)$ for the equation $\Psi(x_1, \dots, x_n) = (y_1, \dots, y_{n+u-r})$ is negligible, and thus that the ciphering function F can be viewed as an surjection from K^n onto K^{n+u-r}.

We will describe in section 5 a general attack on this signature scheme, that is also applicable when u is non-zero, with q^u not too large. Therefore the signature proposed by T.T. Moh in [13, 14] is insecure.

2.4 The TTM encryption system

In the present section, we recall the original description of the TTM cryptosystem, given by T.T. Moh in [13, 14]. This definition of TTM is based on the concept of *tame automorphisms*. As we will see, TTM is a particular case of our general family TPM: it belongs to the family TPM(64, 38, 2,GF(256)).

General Principle
Let K be a finite field (which will be supposed "small" in real applications). We first consider two bijections Φ_2 and Φ_3 from K^{n+v} to K^{n+v}, with $(z_1, \ldots, z_{n+v}) = \Phi_2(x_1, \ldots, x_{n+v})$ and $(y_1, \ldots, y_{n+v}) = \Phi_3(z_1, \ldots, z_{n+v})$ defined by the two following systems of equations :

$$\Phi_2 : \begin{cases} z_1 = x_1 \\ z_2 = x_2 + f_2(x_1) \\ z_3 = x_3 + f_3(x_1, x_2) \\ \quad \vdots \\ z_n = x_n + f_n(x_1, \ldots, x_{n-1}) \\ z_{n+1} = x_{n+1} + f_{n+1}(x_1, \ldots, x_n) \\ \quad \vdots \\ z_{n+v} = x_{n+v} + f_{n+v}(x_1, \ldots, x_{n+v-1}) \end{cases} \qquad \Phi_3 : \begin{cases} y_1 = z_1 + P(z_{n+1}, \ldots, z_{n+v}) \\ y_2 = z_2 + Q(z_{n+1}, \ldots, z_{n+v}) \\ y_3 = z_3 \\ \quad \vdots \\ y_{n+v} = z_{n+v} \end{cases}$$

with $f_2, \ldots, f_{n+v}$ quadratic forms over K, and P, Q two polynomials of degree eight over K.

Φ_2 and Φ_3 are both "tame automorphisms" (see [13, 14] for a definition) and thus are one-to-one transformations. As a result, $(x_1, \ldots, x_{n+v}) \mapsto (y_1, \ldots, y_{n+v}) = \Phi_3 \circ \Phi_2(x_1, \ldots, x_{n+v})$ is also one-to-one and can be described by the following system of equations :

$$\begin{cases} y_1 = x_1 + P\big(x_{n+1} + f_{n+1}(x_1, \ldots, x_n), \ldots, x_{n+v} + f_{n+v}(x_1, \ldots, x_{n+v-1})\big) \\ y_2 = x_2 + f_2(x_1) + Q\big(x_{n+1} + f_{n+1}(x_1, .., x_n), .., x_{n+v} + f_{n+v}(x_1, .., x_{n+v-1})\big) \\ y_3 = x_3 + f_3(x_1, x_2) \\ \quad \vdots \\ y_n = x_n + f_n(x_1, \ldots, x_{n-1}) \\ y_{n+1} = x_{n+1} + f_{n+1}(x_1, \ldots, x_n) \\ \quad \vdots \\ y_{n+v} = x_{n+v} + f_{n+v}(x_1, \ldots, x_{n+v-1}) \end{cases}$$

T.T. Moh found a clever way of choosing P, Q and f_i such that y_1 and y_2 both become *quadratic* functions of $x_1, \ldots, x_n$ when we set $x_{n+1} = \ldots = x_{n+v} = 0$.

Actual Parameters
This paragraph is given in the appendix. T.T. Moh chooses $n = 64$, $v = 36$ and $K = \mathrm{GF}(256)$. As a result, TTM belongs to TPM(64, 38, 2,GF(256)). Applying the formula of section 2.1, the size of the public keys is 214.5 Ko.

3 General Strategy for an Attack on TPM

In the present section, we describe a general strategy to attack a cryptosystem of the TPM Family, when r is “small”. As a result TTM, which belongs to TPM$(64, 38, 2,$GF$(256))$ is threatened by such attacks.

3.1 The MinRank Problem

Let r be an integer and K a field. We denote by MinRank(r) the following problem: given a set $\{M_1, \ldots, M_m\}$ of $n \times n$ matrices whose coefficients lie in K, find at least one m-tuple $(\lambda_1, \ldots, \lambda_m) \in K^m$ such that $\mathrm{Rank}\Big(\sum\limits_{i=1}^{m} \lambda_i M_i\Big) \leq r$.

The MinRank problem was defined and studied in [17] by Shallit, Frandsen and Buss. MinRank generalizes the “Rank Distance Coding” problem (introduced by E. Gabidulin in [10], and considered in [3, 20]), which itself generalizes the “Minimal Weight” problem in error correcting codes (see [1, 19, 2, 11]). In [12], A. Kipnis and A. Shamir exposed a strategy to attack the HFE cryptosystem (invented by J. Patarin, see [15]). They had to face an instance of MinRank(r) with $r = \lceil \log_q n \rceil + 1$. For that purpose, they introduced the “relinearization technique”. But their attack was still not polynomial, unlike here. Note that the idea of finding small ranks was also used by D. Coppersmith, J. Stern and S. Vaudenay (see [6, 7]) in their cryptanalysis of a scheme proposed by A. Shamir in [18].

3.2 Complexity of MinRank

The general MinRank problem has been proven to be NP-complete by Shallit, Frandsen and Buss (see [17]). More precisely, they prove that MinRank(r) NP-complete when $r = n - 1$ (this corresponds to the problem of finding a linear combination of $M_1, \ldots, M_m$ that is singular). The principle of their proof consists in writing any set of multivariate equations as an instance of MinRank. It can be used in the same way to extend their result to the cases $r = n - 2$, $r = n - 3$, $\ldots$ and even $r = n^\alpha$ (when $\alpha > 0$ is fixed). However, there is no such complexity result for smaller values of r. Indeed, as we will see in the following sections, polynomial algorithms can be described to solve the MinRank problem when r is fixed.

3.3 Strategy of attack

We recall that $m = n + u - r$. We suppose $m \leq 2n$, as an encryption function with expansion rate > 2 is unacceptable. Moreover, if $m > \mathcal{O}(n)$, the cryptosystem would be broken by Gröbner bases [8].

In each equation $y_i = x_i + g_i(x_1, \ldots, x_{i-1}\ ; x_{n-r+1}, \ldots, x_n)$ $(1 \leq i \leq n - r)$, the homogeneous part is given by ${}^{\mathrm{t}}X A_i X$, with ${}^{\mathrm{t}}X = (x_1, \ldots, x_n)$, A_i being a (secret) matrix. Similarly, in each public equation $y'_i = P_i(x'_1, \ldots, x'_n)$ is given by ${}^{\mathrm{t}}X' M_i X'$, with ${}^{\mathrm{t}}X' = (x'_1, \ldots, x'_n)$, M_i being a (public) matrix.

The fact that $(x_1, \ldots, x_n) = s(x'_1, \ldots, x'_n)$ and $(y'_1, \ldots, y'_m) = t(y_1, \ldots, y_m)$ implies that there exist an invertible $n \times n$ matrix S and an invertible $m \times m$ matrix T such that:

$$\begin{pmatrix} {}^{\mathrm{t}}(SX')A_1(SX') \\ \vdots \\ {}^{\mathrm{t}}(SX')A_m(SX') \end{pmatrix} = T^{-1} \begin{pmatrix} {}^{\mathrm{t}}X'M_1X' \\ \vdots \\ {}^{\mathrm{t}}X'M_mX' \end{pmatrix}.$$

Let $T^{-1} = (t_{ij})_{1 \leq i,j \leq m}$. We thus have, for any X':

$${}^{\mathrm{t}}X'({}^{\mathrm{t}}SA_iS)X' = {}^{\mathrm{t}}X'\Big(\sum_{j=1}^{m} t_{ij}M_j\Big)X'$$

so that:

$$\forall i,\ 1 \leq i \leq m,\ \sum_{j=1}^{m} t_{ij}M_j = {}^{\mathrm{t}}SA_iS.$$

From the construction of TPM(n, u, r, K), we have Rank$(A_1) \leq r$. Since S is an invertible matrix, we have Rank(A_1) =Rank$({}^{\mathrm{t}}SA_1S)$ and thus Rank$\Big(\sum\limits_{j=1}^{m} t_{1j}M_j\Big) \leq r$, that is precisely an instance of MinRank(r).

Suppose we are able to find (at least) one m-tuple $(\lambda_1, \ldots, \lambda_m)$ such that Rank$\Big(\sum\limits_{j=1}^{m} \lambda_j M_j\Big) \leq r$. With a good probability, we can suppose that:

$$\sum_{j=1}^{m} \lambda_j M_j = \mu\, {}^{\mathrm{t}}SA_1S \qquad (\mu \in K^*).$$

Then we deduce the vector spaces $V_0 = S^{-1}(K^{n-r} \times \{0\}^r)$ (corresponding to $x_{n-r+1} = \ldots = x_n = 0$) and $W_0 = S^{-1}(\{0\}^{n-r} \times K^r)$ (corresponding to $x_1 = \ldots = x_{n-r} = 0$) by simply noticing that $V_0 = \mathrm{Im}\Big(\sum_{j=1}^{m} \lambda_j M_j A_1\Big)$ and $W_0 = \mathrm{Ker}\Big(\sum_{j=1}^{m} \lambda_j M_j A_1\Big)$.

Once we have found V_0 and W_0, we can easily deduce the vector space $V_1 = S^{-1}(\{0\} \times K^{n-r-1} \times \{0\}^r)$ of dimension 1 (corresponding to $x_1 = x_{n-r+1} = \ldots = x_n = 0$) and $W_1 = S^{-1}(K \times \{0\}^{n-r-1} \times K^r)$ (corresponding to $x_2 = \ldots = x_{n-r} = 0$): we just look for coefficients $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ such that the following equation:

$$\sum_{j=1}^{m} \beta_j y'_j = \sum_{i=1}^{n} \alpha_i x_i + \delta,$$

holds for any element of V_0. This can be obtained by simple Gaussian reduction. We also obtain the g_2 quadratic function by Gaussian reduction.

By repeating these steps, we obtain two sequences of vector spaces:

$$V_0 \supseteq V_1 \supseteq V_2 \supseteq \ldots \supseteq V_{n-r-1}$$

$$W_0 \subseteq W_1 \subseteq W_2 \subseteq \ldots \subseteq W_{n-r-1}.$$

At the end, we have completely determined the secret transformations s and t, together with the secret functions g_i. As a result, this algorithm completely breaks the TPM family of cryptosystems (we recovered the secret key).

4 Two attacks on MinRank and TPM

In the previous section, we proved that breaking the TPM family of cryptosystems is easy if we can solve the MinRank(r) problem. This is the point we are interested in, in the present section. Two algorithms will be described.

4.1 The 'Linearity Attack' on MinRank and TTM

In this paragraph, we study the particular case of TTM, as described by T.T. Moh in [13, 14]. In this case, we show that the MinRank(r) problem is easily solved, because of the particular structure of the Q_8 function used in Φ_3.

Description of the Attack

In section 3.3, we proved that an attack can be successfully performed on this cryptosystem, as soon as we can find out the vector spaces $V_0 = S^{-1}(\{0\}^2 \times K^{62})$ (corresponding to $x_1 = x_2 = 0$) and $W_0 = S^{-1}(K^2 \times \{0\}^{62})$ (corresponding to $x_3 = \ldots = x_{64} = 0$). At first sight, the equations giving y_1 and y_2 seem to be quadratic in $(x_1, \ldots, x_{64})$. This leads *a priori* to an instance of MinRank(2).

However, note that the function $x \mapsto x^2$ is linear on $K = \mathrm{GF}(256)$, considered as a vector space of dimension 8 over $F = \mathrm{GF}(2)$. Therefore, considering the equations describing the (secret) Ψ function of TTM[1], if we choose a basis $(\omega_1, \ldots, \omega_8)$ of K over F and write $x_i = x_{i,1}\omega_1 + \ldots + x_{i,8}\omega_8$ $(1 \leq i \leq 64)$, y_1 and y_2 become linear functions of $x_{1,1}, x_{1,2}, \ldots, x_{1,8}, \ldots, x_{64,1}, \ldots, x_{64,8}$. In terms of MinRank, this means that TTM leads to an instance of MinRank(0) for $8n \times 8n$ matrices (instead of an instance of MinRank(2) for $n \times n$ matrices). This leads to the following attack on TTM:

1. Let $x'_i = x'_{i,1}\omega_1 + \ldots + x'_{i,8}\omega_8$ $(1 \leq i \leq 64)$. Rewrite each public equation $y'_i = P_i(x'_1, \ldots, x'_{64})$ as $y'_i = \tilde{P}_i(x'_{1,1}, \ldots, x'_{64,8})$ (with $\tilde{P}_i$ a quadratic polynomial in $64 \times 8 = 512$ variables over $F = \mathrm{GF}(2)$).
2. Find the vector space of the 612-tuples $(\beta_1, \ldots, \beta_{100}, \alpha_{1,1}, \ldots, \alpha_{64,8}) \in K^{612}$ satisfying:
$$\sum_{i=1}^{100} \beta_i y'_i = \sum_{i=1}^{64} \sum_{j=1}^{8} \alpha_{i,j} x'_{i,j}.$$
This can be done by Gaussian reduction. We thus obtain the vector spaces V_0 and W_0 defined above.
3. The remaining part of the attack is exactly the same as in section 3.3.

[1] See (E) in the appendix, in which t_{19} is a linear transformation.

Complexity of the Attack
The main part of the algorithm consists in solving a system of linear equations on 612 variables, by Gaussian reduction. We thus obtain a complexity of approximately 2^{28} elementary operations to break TTM.

4.2 The 'Kernel Attack' on MinRank and TPM

We describe here a new attack on MinRank(r), which works when q^r is small enough.

Description of the Attack (with the same notations as in section 3.3)

1. Choose k random vectors $X'^{[1]}, \ldots, X'^{[k]}$ (with k an integer depending on n and m, that we define below). Since dim $\mathrm{Ker}({}^{\mathrm{t}}SA_1S) = n-$ $\mathrm{Rank}({}^{\mathrm{t}}SA_1S) \geq n - r$, we have the simultaneous conditions $X'^{[i]} \in \mathrm{Ker}({}^{\mathrm{t}}SA_iS)$ $(1 \leq i \leq k)$ with a probability $\geq q^{-kr}$.
2. We suppose we have chosen a "good" set $\{X'^{[1]}, \ldots, X'^{[k]}\}$ of k vectors (*i.e.* such that they all belong to $\mathrm{Ker}({}^{\mathrm{t}}SA_1S)$). Then we can find an m-tuple $(\lambda_1, \ldots, \lambda_m)$ such that, for all i, $1 \leq i \leq k$, $\Big(\sum\limits_{j=1}^{m} \lambda_j M_j\Big)(X'^{[i]}) = 0$. They are solution of a system of kn linear equations in m indeterminates. As a result, if we let $k = \lceil \frac{m}{n} \rceil$, the solution is essentially unique and can be easily found by Gaussian reduction. We thus obtain the two vector spaces $V_0 = S^{-1}(K^{n-r} \times \{0\}^r)$ (corresponding to $x_{n-r+1} = \ldots = x_n = 0$) and $W_0 = S^{-1}(\{0\}^{n-r} \times K^r)$ (corresponding to $x_1 = \ldots = x_{n-r} = 0$).
3. The remaining part of the attack is exactly the same as in section 3.3.

Complexity of the Attack
From the description of the attack, its complexity is easily seen to be $\mathcal{O}(q^{\lceil \frac{m}{n} \rceil r} \cdot m^3)$.

Application to TTM
In the particular case of TTM, we have $q = 256$, $n = 64$, $m = 100$ and $r = 2$.
We thus obtain an attack on TTM in complexity $\mathcal{O}(2^{52})$.

Note: Compared to the 2^{28} of section 4.1, this attack is slower, but it does not make use of any linearity of y_1 and y_2, so that it can also be used to break possible generalizations of TTM, with more general "Q_8 components" (see [4] for examples of Q_8 which provide non linear expressions for y_1 and y_2 over GF(2)).

5 The 'Degenerescence Attack' on TPM signature schemes

We describe here a general attack on TMP signature schemes (recall that such schemes are possible only for $u \leq r$), when q^u is not too large. From the description of the attack, its complexity is easily seen to be $\mathcal{O}(q^u \cdot n^6)$. We use the same notations as in section 3.3. In particular, $m = n + u - r$.

1. We choose a random m-tuple $(\beta_1, \dots, \beta_m) \in K^m$. With a probability q^{-u-1}, we can suppose that $\beta_i P_i$ is a degenerated quadratic polynomial (*i.e.* a quadratic polynomial which can be rewritten with fewer variables after a linear change of variables). The fact that a quadratic polynomial is degenerated can easily be detected: for instance by using its canonical form (see [16] for some other methods).
2. Suppose we have found a "good" m-tuple $(\beta_1, \dots, \beta_m)$. Considering the new set of ($< n$) variables for the quadratic form $\sum_{i=1}^{m} \beta_i P_i$, we deduce easily the vector space $W_{n-r} = S^{-1}(K^{n-r-1} \times \{0\} \times K^r)$.
3. Then we look for a n-tuple $(\alpha_1, \dots, \alpha_n) \in K^n$ and a quadratic function g^{n-r}, such that:
$$\sum_{i=1}^{m} \beta_i y'_i = \sum_{i=1}^{n} \alpha_i x'_i + g_{n-r}(x'_1, \dots, x'_n)$$
is true for any $(x'_1, \dots, x'_n) \in W_{n-r}$. This can be done by Gaussian reduction. We thus obtain the vector space $V_{n-r} = S^{-1}(\{0\}^{n-r-1} \times K \times \{0\}^r)$ and the quadratic polynomial g_{n-r}.
4. The same principle can be repeated $n-r$ times, so as to obtain two sequences of vector spaces:
$$V_{n-r} \subseteq V_{n-r-1} \subseteq \dots \subseteq V_0$$
$$W_{n-r} \supseteq W_{n-r-1} \supseteq \dots \supseteq W_0.$$
At the end, as in the attack described in section 3.3, we have completely determined the secret transformations s and t, together with the secret functions g_i. As a result, this algorithm completely breaks the TPM family in signature mode (we recovered the secret key).

6 Solution to the TTM 2.1 Challenge of US Data Security

In 1997, US Data Security published challenges about TTM (see [21]). They are based on three different versions of TTM in encryption mode, corresponding to different choices of the parameters.

On May 2nd, 2000, we managed to break the second challenge, based on TTM 2.1. As mentioned in [21], "the public-key TTM 2.1 is a block cipher with plaintext block size 64 and ciphertext block size 100. It works on 8 bits finite field (*i.e.*, characters)". The public key can be obtained by approximately 2000 queries to the "encryption oracle". As mentioned in section 2.4, its size is 214.5 Kbytes. By using the general method described in section 4.1, we obtained the following plaintext, which can be easily checked to be the exact solution to this "Contest II" (note that the quotation marks are part of this plaintext):

```
"Tao TTP way BCKP of living hui mountain wen river moon love pt"
```

7 Conclusion

We cryptanalysed a large class of cryptosystems TPM, that includes TTM as it has been described by T.T. Moh [14]. They can be broken in polynomial time, as long as r is fixed. The proposed TTM cryptosystem [14] can be broken in 2^{28}. As an application of our general method, we broke the "TTM 2.1" challenge proposed by US Data Security in October 1997. Even if Q_8 is nonlinear, and since $r = 2$, it is still broken in 2^{52} elementary operations for a 512-bit cryptosystem. There is very little hope that a secure triangular system will ever be proposed.

References

1. E.R. Berlekamp, R.J. McEliece, H.C.A. Van Tilborg, *On the inherent intractability of certain coding problems*, IEEE Transactions on Information Theory, IT-24(3), pp. 384-386, May 1978.
2. F. Chabaud, *Asymptotic analysis of probabilistic algorithms for finding short codewords*, in Proceedings of EUROCODE'92, Udine, Italy, CISM Courses and lectures n° 339, Springer-Verlag, 1993, pp. 217-228.
3. K. Chen, *A new identification algorithm*, Cryptography Policy and Algorithms Conference, LNCS n° 1029, Springer-Verlag, 1996.
4. C. Y. Chou, D. J. Guan, J. M. Chen, *A systematic construction of a Q_{2^k}-module in TTM*, Preprint, October 1999. Available at http://www.usdsi.com/chou.ps
5. D. Coppersmith, S. Winograd, *Matrix multiplication via arithmetic progressions*, J. Symbolic Computation (1990), **9**, pp. 251-280.
6. D. Coppersmith, J. Stern, S. Vaudenay, *Attacks on the Birational Permutation Signature Schemes*, in Advances in Cryptology, Proceedings of Crypto'93, LNCS n° 773, Springer-Verlag, 1993, pp. 435-443.
7. D. Coppersmith, J. Stern, S. Vaudenay, *The Security of the Birational Permutation Signature Schemes*, in Journal of Cryptology, 10(3), pp. 207-221, 1997.
8. N. Courtois, A. Shamir, J. Patarin, A. Klimov, *Efficient Algorithms for solving Overdefined Systems of Multivariate Polynomial Equations*, in Advances in Cryptology, Proceedings of EUROCRYPT'2000, LNCS n° 1807, Springer, 2000, pp. 392-407.
9. H. Fell, W. Diffie, *Analysis of a public key approach based on polynomial substitutions*, in Advances in Cryptology, Proceedings of CRYPTO'85, LNCS n° 218, Springer-Verlag, 1985, pp. 340-349.
10. E.M. Gabidulin, *Theory of codes with maximum rank distance*, Problems of Information Transmission, 21:1-12, 1985.
11. S. Harari, *A new authentication algorithm*, in Coding Theory and Applications, LNCS n° 388, Springer, 1989, pp. 204-211.
12. A. Kipnis, A. Shamir, *Cryptanalysis of the HFE public key cryptosystem*, in Advances in Cryptology, Proceedings of Crypto'99, LNCS n° 1666, Springer, 1999, pp. 19-30.
13. T.T. Moh, *A public key system with signature and master key functions*, Communications in Algebra, 27(5), pp. 2207-2222, 1999. Available at http://www.usdsi.com/public.ps
14. T.T. Moh, *A fast public key system with signature and master key functions*, in Proceedings of CrypTEC'99, International Workshop on Cryptographic Techniques and E-commerce, Hong-Kong City University Press, pp. 63-69, July 1999. Available at http://www.usdsi.com/cryptec.ps

15. J. Patarin, *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms*, in Advances in Cryptology, Proceedings of EUROCRYPT'96, LNCS n° 1070, Springer Verlag, 1996, pp. 33-48.
16. J. Patarin, L. Goubin, *Asymmetric cryptography with S-Boxes*, in Proceedings of ICICS'97, LNCS n° 1334, Springer, 1997, pp. 369-380.
17. J.O. Shallit, G.S. Frandsen, J.F. Buss, *The computational complexity of some problems of linear algebra*, BRICS series report, Aarhus, Denmark, RS-96-33. Available at http://www.brics.dk/RS/96/33
18. A. Shamir, *Efficient Signature Schemes based on Birational Permutations*, in Advances in Cryptology, Proceedings of Crypto'93, LNCS n° 773, Springer-Verlag, 1993, pp. 1-12.
19. J. Stern, *A new identification scheme based on syndrome decoding*, in Advances in Cryptology, Proceedings of CRYPTO'93, LNCS n° 773, Springer-Verlag, 1993, pp. 13-21.
20. J. Stern, F. Chabaud, *The cryptographic security of the Syndrome Decoding problem for rank distance codes*, in Advances in Cryptology, Proceedings of ASIACRYPT'96, LNCS n° 1163, Springer-Verlag, 1985, pp. 368-381.
21. *The US Data Security Public-Key Contest*, available at http://www.usdsi.com/contests.html

Appendix: Actual Parameters for the TTM Cryptosystem

Let Q_8 be the function defined by

$$Q_8(q_1,\ldots,q_{30}) = q_1^8 + q_{29}^4 + q_{30}^2 + [q_2^4 + q_3^2 q_8^2 + q_4^2 q_5^2 + q_6^2 q_{12}^2 + q_7^2 q_{13}^2]$$

$$\times [q_9^4 + (q_{10}^2 + q_{14}q_{15} + q_{18}q_{19} + q_{20}q_{21} + q_{22}q_{24})(q_{11}^2 + q_{16}q_{17} + q_{23}q_{28} + q_{25}q_{26} + q_{13}q_{27})].$$

A straightforward computation gives $Q_8(q_1,\ldots,q_{30}) = t_{19}^2$ as soon as we make the following choices for $q_1,\ldots,q_{30}$:

$q_1 = t_1 + t_2 t_6$	$q_2 = t_2^2 + t_3 t_7$	$q_3 = t_3^2 + t_4 t_{10}$	$q_4 = t_3 t_5$
$q_5 = t_3 t_{11}$	$q_6 = t_4 t_7$	$q_7 = t_4 t_5$	$q_8 = t_7^2 + t_5 t_{11}$
$q_9 = t_6^2 + t_8 t_9$	$q_{10} = t_8^2 + t_{12} t_{13}$	$q_{11} = t_9^2 + t_{14} t_{15}$	$q_{12} = t_7 t_{10}$
$q_{13} = t_{10} t_{11}$	$q_{14} = t_{12}^2 + t_7 t_8$	$q_{15} = t_{13}^2 + t_{11} t_{16}$	$q_{16} = t_{14}^2 + t_{10} t_{12}$
$q_{17} = t_{15}^2 + t_{11} t_{17}$	$q_{18} = t_{12} t_{16}$	$q_{19} = t_{11} t_{12}$	$q_{20} = t_8 t_{13}$
$q_{21} = t_7 t_{13}$	$q_{22} = t_8 t_{16}$	$q_{23} = t_{14} t_{17}$	$q_{24} = t_7 t_{11}$
$q_{25} = t_{12} t_{15}$	$q_{26} = t_{10} t_{15}$	$q_{27} = t_{12} t_{17}$	$q_{28} = t_{11} t_{14}$
$q_{29} = t_{18} + t_1^2$	$q_{30} = t_{19} + t_{18}^2$		

We choose $n = 64$, $v = 36$, and we consider the $t_i = t_i(u_1,\ldots,u_{19})$ $(1 \leq i \leq 19)$ as randomly chosen linear forms (*i.e.* homogeneous polynomials of degree one in $u_1,\ldots,u_{19}$), satisfying the following conditions:

- $t_1(u_1,\ldots,u_{19}) = u_1$;
- $t_{18}(u_1,\ldots,u_{19}) = u_{18}$;
- $t_{19}(u_1,\ldots,u_{19}) = u_{19}$;
- $t_6(u_1,\ldots,u_{19})$, $t_7(u_1,\ldots,u_{19})$, $t_{18}(u_1,\ldots,u_{19})$ and $t_{19}(u_1,\ldots,u_{19})$ depend only on the variables $u_6, u_7, \ldots, u_{17}$,

We thus obtain polynomials $q_i = q_i(u_1, \dots, u_{19})$ $(1 \leq i \leq 30)$ of degree two in $u_1, \dots, u_{19}$. Finally, we choose:

$$\begin{cases}
P(z_{65}, \dots, z_{100}) = Q_8(z_{93}, \dots, z_{100}, z_{73}, \dots, z_{92}, z_{63}, z_{64}) \\
Q(z_{65}, \dots, z_{100}) = Q_8(z_{65}, \dots, z_{92}, z_{61}, z_{62}) \\
f_{61}(x_1, \dots, x_{60}) = q_{29}(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) - x_{61} \\
f_{62}(x_1, \dots, x_{61}) = q_{30}(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) - x_{62} \\
f_{63}(x_1, \dots, x_{62}) = q_{29}(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64}) - x_{63} \\
f_{64}(x_1, \dots, x_{63}) = q_{30}(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64}) - x_{64} \\
f_{65}(x_1, \dots, x_{64}) = q_1(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) \\
\quad \vdots \\
f_{92}(x_1, \dots, x_{91}) = q_{28}(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) \\
f_{93}(x_1, \dots, x_{92}) = q_1(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64}) \\
\quad \vdots \\
f_{100}(x_1, \dots, x_{99}) = q_8(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64})
\end{cases}$$

and randomly chosen quadratic forms for f_i $(2 \leq i \leq 60)$.

Let us denote $\theta : K^{64} \to K^{100}$ the function defined by

$$\theta(x_1, \dots, x_{64}) = (x_1, \dots, x_{64}, 0, \dots, 0).$$

Hence $(x_1, \dots, x_{64}) \mapsto (y_1, \dots, y_{100}) = \Phi_3 \circ \Phi_2 \circ \theta(x_1, \dots, x_{64})$ is given by the following system:

$$(E) \begin{cases}
y_1 = x_1 + [t_{19}(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62})]^2 \qquad (= x_1 + x_{62}^2) \\
y_2 = x_2 + f_2(x_1) + [t_{19}(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64})]^2 \\
\qquad\qquad (= x_2 + f_2(x_1) + x_{64}^2) \\
y_3 = x_3 + f_3(x_1, x_2) \\
\quad \vdots \\
y_{60} = x_{60} + f_{60}(x_1, \dots, x_{59}) \\
y_{61} = q_{29}(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) \qquad (= x_{61} + x_9^2) \\
y_{62} = q_{30}(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) \qquad (= x_{62} + x_{61}^2) \\
y_{63} = q_{29}(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64}) \quad (= x_{63} + x_{10}^2) \\
y_{64} = q_{30}(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64}) \quad (= x_{64} + x_{63}^2) \\
y_{65} = q_1(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) \\
\quad \vdots \\
y_{92} = q_{28}(x_9, x_{11}, \dots, x_{16}, x_{51}, \dots, x_{62}) \\
y_{93} = q_1(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64}) \\
\quad \vdots \\
y_{100} = q_8(x_{10}, x_{17}, \dots, x_{20}, x_{15}, x_{16}, x_{51}, \dots, x_{60}, x_{63}, x_{64})
\end{cases}$$

The Public Key

The user selects a random invertible affine transformation $\Phi_1 : K^{64} \to K^{64}$, and a random invertible affine transformation $\Phi_4 : K^{100} \to K^{100}$, such that the function $F = \Phi_4 \circ \Phi_3 \circ \Phi_2 \circ \theta \circ \Phi_1$ satisfies

$$F(0, \ldots, 0) = (0, \ldots, 0).$$

By construction of F, if we denote $(y'_1, \ldots, y'_{100}) = F(x'_1, \ldots, x'_{64})$, then we have an explicit set $\{P_1, \ldots, P_{100}\}$ of 100 quadratic polynomials in 64 variables, such that:

$$\begin{cases} y'_1 = P_1(x'_1, \ldots, x'_{64}) \\ \quad \vdots \\ y'_{100} = P_{100}(x'_1, \ldots, x'_{64}) \end{cases}$$

This set of 100 polynomials constitutes the public key of the TTM cryptosystem.

Encrypting a message

Given a plaintext $(x'_1, \ldots, x'_{64}) \in K^{64}$, the sender computes $y'_i = P_i(x'_1, \ldots, x'_{64})$ for $1 \leq i \leq 100$ (thanks to the public key) and sends the ciphertext $(y'_1, \ldots, y'_{100})$.

Decrypting a message

Given a ciphertext $(y'_1, \ldots, y'_{100}) \in K^{100}$, the legitimate receiver recovers the plaintext by:

$$(x'_1, \ldots, x'_{64}) = {\Phi_1}^{-1} \circ \pi \circ {\Phi_2}^{-1} \circ {\Phi_3}^{-1} \circ {\Phi_3}^{-1} \circ {\Phi_4}^{-1}(y'_1, \ldots, y'_{100})$$

with $\pi : K^{100} \mapsto K^{64}$ defined by $\pi(x_1, \ldots, x_{100}) = (x_1, \ldots, x_{64})$ and thus satisfies $\pi \circ \theta = \mathrm{Id}$.