Perturbed Hidden Matrix Cryptosystems

Zhiping Wu[1,⋆], Jintai Ding[2], Jason E. Gower[2], and Dingfeng Ye[1,⋆]

[1] State Key Laboratory of Information Security,
Graduate School of Chinese Academy of Sciences,
100039-08, Beijing, China
zpwu@mails.gscas.ac.cn, ydf@is.ac.cn
[2] Department of Mathematical Sciences,
University of Cincinnati,
Cincinnati, OH 45221-0025 USA
{ding, gowerj}@math.uc.edu

Abstract. We apply internal perturbation [3] to the matrix-type cryptosystems $[C_n]$ and HM constructed in [9]. Using small instances of these variants, we investigate the existence of linearization equations and degree 2 equations that could be used in a XL attack. Our results indicate that these new variants may be suitable for use in practical implementations. We propose a specific instance for practical implementation, and estimate its performance and security.

Keywords: public key, multivariate, perturbation, hidden matrix, XL attack.

1 Introduction

Public key cryptography plays an important role in many modern communication systems. In the last few years, great effort has been made to develop cryptosystems based on systems of multivariate polynomials over a finite field. The results of these efforts include C^*, HFE, $[C]$, $[C_n]$ and HM [7, 8, 6, 9]. Recently, the idea of "perturbation" was proposed to improve the security of C^* and HFE [3, 4] without much loss of efficiency. In this paper we study the effect of perturbation on the matrix-type schemes $[C_n]$ and HM.

To construct $[C_n]$ or HM, we begin by choosing secret invertible affine transformations $s : K^{n^2} \longrightarrow \mathcal{M}_n(K)$ and $t : \mathcal{M}_n(K) \longrightarrow K^{n^2}$, where K is a finite field and $\mathcal{M}_n(K)$ is the set of $n \times n$ matrices with entries in K. If we have an "invertible" quadratic map $g : \mathcal{M}_n(K) \longrightarrow \mathcal{M}_n(K)$, we can build a cipher for encryption as follows: $x \overset{s}{\longmapsto} A \overset{g}{\longmapsto} g(A) \overset{t}{\longmapsto} y$, where $x, y \in K^{n^2}$, $A \in \mathcal{M}_n(K)$, and K^{n^2} is the plaintext/ciphertext space. If the inverse of the mapping g can be computed in polynomial time then the decryption can be performed efficiently. However, $[C_n]$ is vulnerable to the linearization attack, and HM may be vulner-

[⋆] Supported by Natural Science Foundation of China No. 60473026.

O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481, pp. 595–602, 2005.

able to XL-type attacks [1] due to that fact that such systems may produce a large number of new quadratic equations.

To create perturbation we choose a set of linear polynomials $z_j = \sum \alpha_{ij} x_i + \beta_j$ (for $j = 1, \ldots, r$) in the variables x_i of the original system such that the $z_j - \beta_j$ are linearly independent. A set of randomly chosen secret quadratic polynomials in the z_j are added to $[C_n]$ to produce the first PHM system. Similarly, randomly chosen secret linear and quadratic polynomials in the z_j are applied to HM to produce the second PHM system. For several small instances of both variants, we made a direct search for potentially fatal linearization and quadratic equations. Our results indicate that for proper choices of parameters these variants are very likely to be resistant to linearization and XL-type attacks.

In the first section we introduce $[C_n]$ and HM, along with the known attacks on these systems. We then describe in Section 3 a method for constructing two new variants using perturbation. In Section 4 we analyze the security of these new variants against the known attacks, and then in Section 5 we use this analysis to suggest some choices of parameters for use in practical implementations. We summarize our work in Section 6.

2 Hidden Matrix Cryptosystems

The first multivariate cryptosystem based on matrices, $[C]$, was proposed by Imai and Matsumoto [6]. This system and its generalization, $[C_n]$, were defeated by Patarin, Goubin and Courtois using linearization equations [9]. In this same paper, they suggested an improved scheme that they named the Hidden Matrix (HM) cryptosystem. Though HM is resistant to the linearization attack, it is sometimes possible to generate several new quadratic equations that can be used in a XL attack.

2.1 Description of $[C_n]$ and HM

Let K be a finite field of cardinality $q = 2^m$ and let $\mathcal{M}_n(K)$ denote the set of $n \times n$ matrices with entries in K. Recall that $\mathcal{M}_n(K)$ can be considered as a vector space of dimension n^2 over K. Plaintext and ciphertext are elements in K^{n^2}.

Public/Private Keys: The private key consists of the invertible affine transformations $s : K^{n^2} \longrightarrow \mathcal{M}_n(K)$ and $t : \mathcal{M}_n(K) \longrightarrow K^{n^2}$. The public key includes the field structure of K, and $f : K^{n^2} \longrightarrow K^{n^2}$, where $f(x) = (t \circ g \circ s)(x) = (f_1, \ldots, f_{n^2})$ and $g : \mathcal{M}_n(K) \longrightarrow \mathcal{M}_n(K)$ is quadratic (hence the f_i are quadratic as well). If $g(x) = x^2$, then we have $[C_n]$; if $g(x) = x^2 + Mx$, for some nonzero secret matrix M, then we have HM.

Encryption/Decryption: For any plaintext $\left(x'_1, \ldots, x'_{n^2}\right)$, the corresponding ciphertext $\left(y'_1, \ldots, y'_{n^2}\right)$ can be computed by $y'_i = f_i\left(x'_1, \ldots, x'_{n^2}\right)$. To decrypt a given ciphertext $y' \in K^{n^2}$, we solve the equation $g(A) = B$, where $B = t^{-1}(y')$, and then compute the plaintext as $x' = s^{-1}(A)$. For more about the decryption of $C[n]$ and HM, see [9].

2.2 Attacks on $[C_n]$ and HM

Patarin, Goubin and Courtois used the linearization attack to defeat $[C_n]$, and then suggested HM as a possible improvement. However, the improved scheme also has a potential defect that frequently allows attackers to produce many new quadratic equations satisfied by the plaintext/ciphertext pairs.

Linearization Attack: In $[C_n]$, if $A = s(x_1, \ldots, x_{n^2})$, and $B = g(A) = A^2$, then we have $AB = BA$. This equation can be used to generate linearization equations

$$\sum a_{ij} x_i y_j + \sum b_i x_i + \sum c_j y_j + d = 0 \tag{1}$$

satisfied by any plaintext/ciphertext pair. If enough of these equations can be found then we can find the plaintext for a given ciphertext.

Degree 2 Equation Attack: The authors in [9] noticed that for HM we have the equation $AB - BA = AMA - MA^2$, where $g(A) = A^2 + MA$. This yields n^2 quadratic equations of the form:

$$\sum \alpha_{ij} x_i x_j + \sum \beta_{ij} x_i y_j + \sum \gamma_i x_i + \sum \delta_i y_i + \mu = 0\ , \tag{2}$$

and so for a given ciphertext we can generate n^2 quadratic equations satisfied by the plaintext. These “new” quadratic equations can be combined with the public key equations and used in a XL-type attack. We refer to this generation of new quadratic equations as a *degree 2 equation attack.*

3 Perturbed Hidden Matrix Cryptosystems

$[C_n]$ and HM may not be suitable for practical use due to the attacks outlined in the previous section. In this section we show how to apply the idea of perturbation to these two schemes as a way to create resistance to these attacks.

3.1 Perturbation of $[C_n]$

Let r be a small positive integer and $z_j = \sum \alpha_{ij} x_i + \beta_j$ (for $j = 1, \ldots, r$) be randomly chosen degree 1 polynomials in the x_i over K such that the $z_j - \beta_j$ are linearly independent. Let $Z : K^{n^2} \longrightarrow K^r$ be the map defined by $Z(x_1, \ldots, x_{n^2}) = (z_1(x_1, \ldots, x_{n^2}), \ldots, z_r(x_1, \ldots, x_{n^2}))$. Randomly choose n^2 quadratic polynomials $f_1, \ldots, f_{n^2}$ in the variables $z_1, \ldots, z_r$, and define the map $f : K^r \longrightarrow K^{n^2}$ by $f(z_1, \ldots, z_r) = (f_1(z_1, \ldots, z_r), \ldots, f_{n^2}(z_1, \ldots, z_r))$. Let $u : K^{n^2} \longrightarrow \mathcal{M}_n(K)$ be another secret invertible affine transformation and compute $B' = u \circ f$. Let $P = \{(\lambda, \mu) : \lambda \in (u \circ f)(K^r),\ \mu = (u \circ f)^{-1}(\lambda)\}$. The set P is called the *perturbation set.* We construct the first perturbed hidden matrix (PHM) scheme as illustrated in Figure 1, where we define $\bar{B} = B + B'$. We say that that $\bar{B}$ is the *perturbation* of B by B', and that the number r is the *perturbation dimension.*

Public/Private Keys: The private key includes the three affine transformations s, u, and t; the set of degree 1 polynomials $z_1, \ldots, z_r$; and the set P, or

$$\begin{tikzcd}
x \arrow[r, "s"] \arrow[dd, "Z"'] & A \arrow[r] & B \arrow[d] & \\
 & & \bar{B} \arrow[r, "t"] & y \\
z \arrow[r] & f \arrow[r, "u"] & B' \arrow[u] &
\end{tikzcd}$$

Fig. 1. Construction of the first PHM

equivalently, the set of the polynomials $f_i\left(z_1, \ldots, z_r\right)$. The public key includes the field structure of K and the n^2 quadratic polynomials $y_1, \ldots, y_{n^2}$.

Encryption/Decryption: Given a plaintext message $x' = \left(x'_1, \ldots, x'_{n^2}\right)$, the ciphertext is $y' = \left(y'_1, \ldots, y'_{n^2}\right)$, where $y'_i = y_i\left(x'_1, \ldots, x'_{n^2}\right)$. To decrypt a given ciphertext $\left(y'_1, \ldots, y'_{n^2}\right)$, we first compute $\bar{B} = t^{-1}\left(y'_1, \ldots, y'_{n^2}\right)$. For each $(\lambda, \mu) \in P$ we compute $\left(x'_{\lambda 1}, \ldots, x'_{\lambda n^2}\right) = (g \circ s)^{-1}\left(\bar{B} - \lambda\right)$, and then check if $Z\left(x'_{\lambda 1}, \ldots, x'_{\lambda n^2}\right)$ is the same as the corresponding μ. If it is not then we discard it; otherwise $\left(x'_{\lambda 1}, \ldots, x'_{\lambda n^2}\right)$ may be the plaintext. It is possible that there may be more than one candidate for the plaintext. However, we can use the same technique suggested in [8] to find the true plaintext.

3.2 Perturbation of HM

First let $h_1, \ldots, h_{n^2}$ be randomly chosen degree 1 polynomials in the variables $z_1, \ldots, z_r$, where the z_i are as above, which defines a map $h : K^r \longrightarrow K^{n^2}$. Let $v : K^{n^2} \longrightarrow \mathcal{M}_n(K)$ be an invertible affine transformation and define $A' = v \circ h$. Let $f_1, \ldots, f_{n^2}$ be randomly chosen quadratic polynomials in the variables $z_1, \ldots, z_r$, which defines a map $f : K^r \longrightarrow K^{n^2}$. We choose $u : K^{n^2} \longrightarrow \mathcal{M}_n(K)$ to be another secret invertible affine transformation and define $A'' = u \circ f$. Let $P = \{(\lambda_h, \lambda_f, \mu) : \lambda_h \in (v \circ h)(K^r),\ \lambda_f \in (u \circ f)(K^r),\ \mu = (v \circ h)^{-1}(\lambda_h) \cap (u \circ f)^{-1}(\lambda_f)\}$. We construct the second PHM scheme as defined in Figure 2, where

$$\begin{tikzcd}
x \arrow[r, "s"] \arrow[d] & A \arrow[r] & B \arrow[r] & \bar{B} \arrow[r, "t"] & y \\
z \arrow[r] \arrow[dr] & h \arrow[r, "v"] & A' \arrow[u] & & \\
 & f \arrow[r, "u"] & A'' \arrow[uur] & &
\end{tikzcd}$$

Fig. 2. Construction of the second PHM

$\bar{B} = g(A) + A'' = A^2 + A'A + A''$ is the perturbation by A' and A'', and $g(x) = x^2 + A'x$. Here we must include u, v, h and f in the private key, and modify the decryption process as follows. For each $(\lambda_h, \lambda_f, \mu) \in P$, compute $(x_{\lambda 1}, \ldots, x_{\lambda n^2}) = (g \circ s)^{-1}\left(\bar{B} - \lambda_f\right)$; in other words, solve the equation $\bar{B} - \lambda_f = g(A) = A^2 + \lambda_h A$ for A, where λ_h and λ_f are known, and then find $s^{-1}(A)$. Check if $Z\left(x_{\lambda 1}, \ldots, x_{\lambda n^2}\right)$ is the same as the corresponding μ. If it is not then discard it; otherwise $(x_{\lambda 1}, \ldots, x_{\lambda n^2})$ may be the plaintext.

4 Security of PHMs

In this section, we investigate the security of the two PHM schemes. The existing attacks on hidden matrix cryptosystems mainly use either the linearization attack or the degree 2 equation attack using the XL method (see [9]). We now consider the application of these attacks to the PHM schemes.

4.1 Linearization Attacks on PHM

We can obtain linearization equations to attack $[C_n]$ from $BA = AB$. The analogous equation that we should consider in either of the PHM system is $\bar{B}A - A\bar{B} = 0$. Of course, this equation need not be true; however, we may be able to find non-trivial linear relations among the n^2 entries of the left-hand side of this equation, which could potentially yield many linearization equations. Even if this is impossible, we are still not guaranteed that linearization equations do not exist. Therefore, in order to test the two PHM schemes for the existence of linearization equations, we search directly for all equations of the form of Equation (1), in the variables a_{ij}, b_i, c_i, d, which hold for all plaintext/ciphertext pairs $x = (x_1, \ldots, x_{n^2}), y = (y_1, \ldots, y_{n^2})$, for small values of n and r. Table 1 summarizes our findings for 100 randomly chosen instances for each choice of parameters (n, r) with $3 \leq n \leq 6$ and $3 \leq r \leq 9$. The entry in the n^{th} row and r^{th} column is the probability that a particular instance with parameters (n, r) had no linearization equations.

Table 1. Linearization Attack Failure Probabilities

First PHM							
$n\backslash r$	3	4	5	6	7	8	9
3	0.39	0.49	0.73	0.80	0.90	0.96	0.98
4	0.30	0.50	0.77	0.91	0.95	0.97	0.99
5	0.98	1	1	1	1	1	1
6	1	1	1	1	1	1	1
Second PHM							
$n\backslash r$	3	4	5	6	7	8	9
3	0.84	0.88	0.95	0.97	0.97	0.99	0.99
4	0.88	0.98	0.97	1	1	1	1
5	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1

4.2 Degree 2 Equation Attack on PHM

In order to resist the degree 2 equation attack, we need to show that it is not easy to generate new quadratic equations. First notice that if the linear space spanned by the degree 3 terms in the entries of $\bar{B}A - A\bar{B}$ has maximum dimension of $n^2 - 1$, then no new degree 2 equations can be found from linear combinations of the degree 3 entries. (Note that the -1 comes from the trivial relations derived from the trace of $\bar{B}A - A\bar{B}$.) Table 2 shows the probability that the linear space

Table 2. First Degree 2 Equation Attack Failure Probabilities

First PHM							
$n\backslash r$	3	4	5	6	7	8	9
3	0.18	0.48	0.73	0.79	0.88	0.98	0.98
4	0.17	0.53	0.69	0.83	0.92	0.97	1
5	0.15	0.54	0.65	0.89	0.92	0.96	1
6	0.08	0.49	0.66	0.81	0.95	0.97	0.98
Second PHM							
$n\backslash r$	3	4	5	6	7	8	9
3	0.95	0.97	0.99	0.99	1	1	1
4	0.94	0.99	0.99	0.99	1	1	1
5	0.93	0.95	0.99	1	1	1	1
6	0.93	0.96	1	1	1	1	1

spanned by the degree 3 terms in $\bar{B}A - A\bar{B}$ is of maximum dimension for the instances considered in the linearization attack of the previous section.

Once again we note that even if we cannot use $\bar{B}A - A\bar{B}$ to find new quadratic equations this does not imply that there are no new quadratic equations. Therefore we performed experiments to directly check whether or not there are new nontrivial solutions to Equation (2) in the variables $\alpha_{ij}, \beta_{ij}, \gamma_i, \delta_i, \mu$. Table 3 shows the probability that the above equation has no new nontrivial solutions for the instances considered in the linearization attack of the previous section.

Table 3. Second Degree 2 Equation Attack Failure Probabilities

First PHM							
$n\backslash r$	3	4	5	6	7	8	9
3	0	0.03	0.03	0.16	0.18	0.40	0.63
4	0	0.05	0.18	0.37	0.53	0.72	0.84
5	0.69	0.87	0.95	1	1	1	1
6	1	1	1	1	1	1	1
Second PHM							
$n\backslash r$	3	4	5	6	7	8	9
3	0.19	0.35	0.54	0.66	0.63	0.77	0.82
4	0.59	0.86	0.93	0.99	1	1	1
5	1	1	1	1	1	1	1
6	1	1	1	1	1	1	1

5 A Practical Implementation

We note that when $r = 0$, the first and second PHM reduce to $[C_n]$ and HM, respectively. On the other hand, any system with $r = n^2$ would simply be a system of n^2 randomly chosen quadratic polynomials. Since the decryption is slower by a multiple of q^r, we must not choose r too large. For any given choice of n and r, we suggest using the second PHM rather than the first due to the former's superior resistance to both linearization and degree 2 attacks.

Parameters and Security: With $q = 2$ (i.e., $m = 1$), our experiments suggest that if we take $n = 11$, then $r = 5$ should be large enough so that the probability that either a linearization or degree 2 attack will be successful is extremely small. Based on preliminary experiments using F_4 [5], we project that the time and memory requirements of a Gröbner basis attack will be prohibitively large, and that implementations of the second PHM with $n = 11$ and $r = 5$ will enjoy a security level of 2^{121} 3-DES.

Public/Private Key Size: An implementation of the second PHM with parameters $q = 2, n = 11$ and $r = 5$ will have a public key which consists of 121 quadratic polynomials. Each polynomial has $\binom{121}{2} = 7,260$ quadratic terms, 121 linear terms, and one constant term, so the public key size is roughly 109 KB. The private key includes the four affine transformations s, t, u, and v, the perturbation vector z, and the perturbation set P. The four affine maps and their inverses together require $121 \cdot 121 \cdot 2 \cdot 4 = 117,128$ bits of storage, the five linear polynomial components of z require $(121 + 1) \cdot 5 = 610$ bits of storage, and P requires $32 \cdot (5 + 2 \cdot 121) = 7904$ bits of storage. Therefore the private key requires roughly 15.3 KB of storage.

Encryption/Decryption Computational Complexity: For encryption, we need to compute the value of 121 quadratic polynomials for a given plaintext $x' = (x'_1, \ldots, x'_{121})$. Calculating the value of each polynomial needs 14,641 multiplications and 122 additions when we rewrite each quadratic polynomial as $\sum x_i \left(b_i + \sum a_{ij} x_j\right) + c$. The decryption will be slower than it is for HM due to the perturbation set P. If ν is the time required to compare the value of $Z(x'_1, \ldots, x'_{n^2})$ with μ in the decryption step, then the extra time spent will be at most 32ν, though we expect it to be much smaller on average.

6 Conclusion

In this paper, we illustrate how to perturb the matrix-type cryptosystems $[C_n]$ and HM. Computer experiments with small parameter choices indicate that the resulting two variants seem to be very resistant to both linearization attacks and degree 2 attacks. We propose a practical implementation scheme for the second PHM system with an estimated security of 2^{121} 3-DES. We note in passing that these new variants can be easily modified for use as signature schemes. We believe that our results, though experimental in nature, are promising and warrant further investigation.

Acknowledgements

We would like to thank the anonymous referees for their valuable comments and suggestions.

References

1. N. Courtois, A. Klimov, J. Patarin and A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In *EUROCRYPT 2000*, LNCS 1807:392–407.
2. N. Courtois and J. Patarin. About the XL Algorithm over $GF(2)$. In *CT-RSA 2003*, LNCS 2612:141–157.
3. J. Ding. A New Variant of the Matsumoto-Imai Cryptosystem Through Perturbation. In *PKC 2004*, LNCS 2947:305–318.
4. J. Ding. Cryptanalysis of HFEv and Internal Perturbation of HFE. In *PKC 2005*, LNCS 3386:288–301.
5. J.-C. Faugère. A New Efficient Algorithm for Computing Gröbner Bases (F_4). In *Journal of Applied and Pure Algebra*, 139:61–88, June 1999.
6. H. Imai and T. Matsumoto. Algebraic Methods for Constructing Asymmetric Cryptosystems. In *AAECC-3*, LNCS 229:108–119, 1985.
7. T. Matsumoto and H. Imai. Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In *EUROCRYPT 1988*, LNCS 330:419–453.
8. J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *EUROCRYPT 1996*, LNCS 1070:33–48.
9. J. Patarin, L. Goubin and N. Courtois. C^*_{-+} and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai. In *ASIACRYPT 1998*, LNCS 1514:35–50.