Breaking the Hidden Irreducible Polynomials Scheme

Christian Eder

Department of Mathematics

TU Kaiserslautern, Germany

ederc@mathematik.uni-kl.de

November 5, 2019

Abstract

In [1] Gómez describes a new public key cryptography scheme based on ideas from multivariate public key cryptography using hidden irreducible polynomials. We show that the scheme's design has a flaw which lets an attacker recover the private key directly from the public key.

***Keywords*—** Multivariate Public-key Cryptography, Univariate Polynomial Factorization

1 Introduction

For several decades public-key cryptography schemes whose security based on the hardness of solving multivariate polynomial systems over finite fields. One of the first such schemes was in 1988 C^* by Matsumoto and Imai [3], which was broken by Patarin in 1995 [4]. From this point onwards many multivariate schemes, mostly signature schemes, evolved, for example, HFE [5], FLASH [6], UOV [2]. These and other systems come in many different variations of these systems. Especially multivariate signature schemes are stand the test of time, some of them also part of the ongoing post-quantum standardization process by the National Institute of Standards and Technology (NIST).

Still, designing multivariate encryption schemes is a harder task since most of the proposed systems have been successully analyzed and broken. In [1] Gómez describes a new public key cryptography scheme based on ideas from multivariate public key cryptography using hidden irreducible polynomials. The fundamental idea behind the system is polynomial multiplication and factorization.

1.1 Our Contribution

We show that the design of the Hidden Irreducible Polynomials scheme itself reveals the private key which leads to a full break. We state two possible attacks.

1.2 Organization

The paper is organized as follows: In Section 2 we shortly review the Hidden Irreducible Polynomials scheme. In Section 3 we show how the private key is extracted from the construction of the scheme. We then give two possible attacks: One based on linear algebra, the other one directly reading off the private key from the public one. In Section 4 we conclude the full break of the scheme.

2 Description of the scheme

We start with a short review of the construction of the Hidden Irreducible Polynomials scheme:

Definition 1.

1. *Let p be a prime number, for a given $m \in \mathbb{N}$ we set $q := p^m$.*[1] *We consider the field extension $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/h(x) =: K$ for some irreducible polynomial $h \in \mathbb{F}_q[x]$ of degree $\deg(h) = n$.*
2. *We fix two polynomials*

$$\begin{aligned} f(x) &:= y_1 + y_2 x + \cdots + y_{k+1}x^k, \\ g(x) &:= y_{k+2} + y_{k+3}x + \cdots + y_{2(k+1)}x^k. \end{aligned}$$

   in K of degree $\deg(f) = \deg(g) = k$ for some prime number $k \in \mathbb{N}$ such that $2k < n - 1$ and $y_i \in \mathbb{F}_q$ for all $1 \leq j \leq 2(k+1)$.[2]
3. *The **private map** $\mathfrak{F}$ is given by*

$$\begin{aligned} \mathfrak{F}: \quad \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n}, \\ (f(x), g(x)) &\mapsto f(x) \cdot g(x). \end{aligned}$$

4. *For $u(x) = c_0 + c_1 x + \cdots c_{n-1}x^{n-1} \in K$ we define the one-to-one map*

$$\begin{aligned} \varphi: \quad K &\to \mathbb{F}_q^n, \\ u(x) &\mapsto (c_0, \ldots, c_{n-1}). \end{aligned}$$

5. *$T \in \mathrm{GL}\left(\mathbb{F}_q, (2k+1) \times (2k+1)\right)$ denotes the transformation matrix.*

[1] In [1] the author uses n instead of m. Since m denotes also a different property in [1], we made the distinction by using different letters.

[2] In [1] the authors uses $p(x)$ and $q(x)$ instead of $f(x)$ and $g(x)$. Again, $p(x)$ and $q(x)$ denote in [1] other polynomials.

6. *The **public map** $\mathfrak{P}$ is given by:*

$$\begin{array}{rccc} \mathfrak{P}: & \mathbb{F}_q^{2(k+1)} & \to & \mathbb{F}_{q^n}, \\ & \left(t_1, \ldots, t_{2(k+1)}\right) & \mapsto & \sum_{i=0}^{2k} p_i \left(t_1, \ldots, t_{2(k+1)}\right) x^i. \end{array}$$

where the $p_i \in \mathbb{F}_q[y_1, y_2, \ldots, y_{2(k+1)}]$ are constructed via

$$\begin{gathered} \left(p_1 \left(y_1, \ldots, y_{2(k+1)}\right), \ldots, p_{2k+1} \left(y_1, \ldots, y_{2(k+1)}\right), 0, \ldots, 0\right) \\ := \\ \varphi^{-1} \circ T \circ \varphi \circ \mathfrak{F}\left(f(x), g(x)\right) \end{gathered}$$

with $n - 2k - 1$ zeroes at the end.

Applying the scheme for encryption and decryption one needs to implement the following steps. Here we assume that Alice generates the private and the public map and distributes the public map. Bob now uses the public map to encrypt a message to Alice, which she then decrypts using the private map.

Definition 2.

1. *With the above definitions Alice would create the private map $\mathfrak{F}$, construct a random transformation matrix T and generate from these a corresponding public map $\mathfrak{P}$.*
2. *Bob is able to use Alice's public map $\mathfrak{P}$: He constructs two irreducible polynomials $p, q \in K$ both of degree k. Bob wants to share p and q with Alice secretly.*
3. *Using the map φ, Bob can map the coefficients of p and q to coefficient vectors in $\mathbb{F}_q^{k+1} \subset \mathbb{F}_q^n$. Concatenating $\varphi(p)$ and $\varphi(q)$ we receive a coefficient vector $v := \varphi(p)||\varphi(q) \in \mathbb{F}_q^{2(k+1)}$. In other words, the information of both polynomials is encoded in one long vector of corresponding coefficients.*
4. *Bob uses $\mathfrak{P}$, the system of quadratic multivariate polynomial equations. Each polynomial p_i in $\mathfrak{P}$ takes $2(k+1)$ variables, so Bob applies v to all the p_i and gets an element $w := \mathfrak{P}(v) \in \mathbb{F}_q^{2k+1}$. Bob further applies φ^{-1} to w to receive the encrypted message $z \in K$, a univariate polynomial of degree $\deg(z) = 2k$.*
5. *Bob sends z to Alice. Alice first uses φ to get the coefficient vector of z. Then she can apply the inverse of the privately known transformation matrix T. Finally, applying φ^{-1}, she receives a polynomial $r \in K$ of degree $\deg(r) = 2k$. This univariate polynomial can now be factorized, and Alice receives Bob's input polynomials p, q.*

Remark 3.

1. *One would assume due to the idea of the scheme, that p and q are multiplied to a polynomial $r(x) = p(x) \cdot q(x)$ and then v is the coefficient vector of r. This is done under the hood, as $\mathfrak{F}$ is nothing else but multiplying the input polynomials which are encoded as one long coefficient vector.*
2. *Note that the factorization step also does not hold any private information: If the factorization would not be efficient, Alice could not recover Bob's p and q. So anyone who gets r also gets p and q.*

3 Breaking the scheme

In the last section we gave a review on how the hidden irreducible polynomials scheme is constructed, how encryption and decryption works. There are two main observations:

Remark 4.

1. *f, g, the ingredients to construct the private map are known and unique once k is fixed. The coefficients y_i cannot be further specified but need to be parameters in order to be used in the public map $\mathfrak{P}$ as the variables of the multivariate quadratic polynomials p_i. So $\mathfrak{F}$ is known to anybody.*
2. *Looking again at Step 5 in Definition 2 Alice only uses φ (publicly known) and T to receive r. Thus the only secret part of the scheme is T, an invertible matrix*

This leads to the first possible attack.

Attack 5 (Using linear algebra only)**.** *By definition it holds that*

$$\mathfrak{P} = \varphi^{-1} \circ T \circ \varphi \circ \mathfrak{F}\,.$$

Thus we can get T via linear algebra computing

$$\varphi \circ \mathfrak{P} = T \circ (\varphi \circ \mathfrak{F})\,.$$

Here, all data besides T is publicly known.

It turns out that we do not even need to relinearize the system via defining new variables $y_{i,j} := y_i y_j$ and solve the system of linear equations, we can do even better.

We have seen in Definition 1.3 that $\mathfrak{F}$ consists of the product r of the two arbitrary univariate polynomials f and g, both of degree k, so we get

$$\begin{aligned} r(x) &= y_{1,k+2}x^0 \\ &+ \left(y_{1,k+3} + y_{2,k+2}\right)x^1 \\ &+ \left(y_{1,k+4} + y_{2,k+3} + y_3, k+2\right)x^2 \\ &+ \vdots \\ &+ \left(y_{k,2k+2} + y_{k+1,2k+1}\right)x^{2k-1} \\ &+ y_{k+1,2k+2}x^{2k}. \end{aligned}$$

For the sake of an easier notation let us define the following notion.

Definition 6. *Let $k \in \mathbb{N}$.. We define the m**th coefficient sum** to be*

$$Y_m := \sum_{(i,j)\in I_m} y_{i,j}$$

such that $I_m := \{(i,j) \mid 1 \le i \le k+1, k+2 \le j \le 2k+2, i+j = m+k+2\}$ for $1 \le m \le 2k+1$.

With Definition 6 we can represent $r(x)$ in a more natural way:

$$r(x) = \sum_{i=0}^{2k} Y_{i+1} x^i. \tag{1}$$

Even more, we can easily proof the following statement.

Lemma 7. $I_\ell \cap I_m = \emptyset \iff \ell \neq m$.

Proof. Both directions follow directly by the structure of f and g (Definition 1.2) and the definition of $r(x) = f(x) \cdot g(x)$. □ □

This new representation of the main data structures of the hidden irreducible polynomials scheme leads to another attack.

Attack 8 (Reading off T from $\mathfrak{P}$)**.** *Applying φ to $\mathfrak{F}$ we get with Equation 1*

$$\varphi \circ \mathfrak{F} = \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_{2k} \\ Y_{2k+1} \end{pmatrix} \in \mathbb{F}_q^{2k+1} \subset \mathbb{F}_q^n.$$

By Definition 1(6) we have that $\varphi \circ \mathfrak{P} = T \circ \varphi \circ \mathfrak{F}$. Thus rewriting $\varphi \circ \mathfrak{P}$ using the notation of coefficient sums (Definition 6) we get

$$\varphi \circ \mathfrak{P} = \begin{pmatrix} \sum_{\ell=1}^{2k+1} t_{1,\ell} Y_\ell \\ \vdots \\ \sum_{\ell=1}^{2k+1} t_{2k+1,\ell} Y_\ell \end{pmatrix}.$$

Since by Lemma 7 all I_ℓ are disjoint, given $\mathfrak{P}$, none of the appearing coefficients in front of the Y_ℓ are interfered, but exactly the matrix entries $t_{i,j}$. Thus, we can directly read off T from $\mathfrak{P}$.

Let us recall the example given in Section 6 in [1] to show how Attack 8 works:

Example 9. *In the given example we have $q = 2$ and $k = 7$. T is thus given as the 15×15 $\mathbb{F}_2$-matrix*

$$T = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Looking at $\mathfrak{P}$ *we get the following system of* 15 *multivariate quadratic equations in the variables* $y_1, \ldots, y_{16}$*:*

$$\begin{aligned}
&y_2y_9 + y_4y_9 + y_8y_9 + y_1y_{10} + y_3y_{10} + y_7y_{10} + y_2y_{11} + y_6y_{11} + y_8y_{11} \\
&+y_1y_{12} + y_5y_{12} + y_7y_{12} + y_8y_{12} + y_4y_{13} + y_6y_{13} + y_7y_{13} + y_8y_{13} + y_3y_{14} \\
&+y_5y_{14} + y_6y_{14} + y_7y_{14} + y_8y_{14} + y_2y_{15} + y_4y_{15} + y_5y_{15} + y_6y_{15} + y_7y_{15} \\
&+y_8y_{15} + y_1y_{16} + y_3y_{16} + y_4y_{16} + y_5y_{16} + y_6y_{16} + y_7y_{16} + y_8y_{16}, \\
&y_1y_9 + y_2y_9 + y_3y_9 + y_4y_9 + y_5y_9 + y_8y_9 + y_1y_{10} + y_2y_{10} + y_3y_{10} \\
&+y_4y_{10} + y_7y_{10} + y_8y_{10} + y_1y_{11} + y_2y_{11} + y_3y_{11} + y_6y_{11} + y_7y_{11} + y_8y_{11} \\
&+y_1y_{12} + y_2y_{12} + y_5y_{12} + y_6y_{12} + y_7y_{12} + y_8y_{12} + y_1y_{13} + y_4y_{13} + y_5y_{13} \\
&+y_6y_{13} + y_7y_{13} + y_3y_{14} + y_4y_{14} + y_5y_{14} + y_6y_{14} + y_2y_{15} + y_3y_{15} + y_4y_{15} \\
&+y_5y_{15} + y_8y_{15} + y_1y_{16} + y_2y_{16} + y_3y_{16} + y_4y_{16} + y_7y_{16}, \\
&\vdots \\
&y_1y_9 + y_4y_9 + y_6y_9 + y_8y_9 + y_3y_{10} + y_5y_{10} + y_7y_{10} + y_2y_{11} + y_4y_{11} \\
&+y_6y_{11} + y_8y_{11} + y_1y_{12} + y_3y_{12} + y_5y_{12} + y_7y_{12} + y_8y_{12} + y_2y_{13} + y_4y_{13} \\
&+y_6y_{13} + y_7y_{13} + y_1y_{14} + y_3y_{14} + y_5y_{14} + y_6y_{14} + y_2y_{15} + y_4y_{15} + y_5y_{15} \\
&+y_8y_{15} + y_1y_{16} + y_3y_{16} + y_4y_{16} + y_7y_{16} + y_8y_{16}, \\
&y_1y_9 + y_2y_9 + y_4y_9 + y_5y_9 + y_6y_9 + y_7y_9 + y_1y_{10} + y_3y_{10} + y_4y_{10} \\
&+y_5y_{10} + y_6y_{10} + y_2y_{11} + y_3y_{11} + y_4y_{11} + y_5y_{11} + y_8y_{11} + y_1y_{12} + y_2y_{12} \\
&+y_3y_{12} + y_4y_{12} + y_7y_{12} + y_1y_{13} + y_2y_{13} + y_3y_{13} + y_6y_{13} + y_8y_{13} + y_1y_{14} \\
&+y_2y_{14} + y_5y_{14} + y_7y_{14} + y_1y_{15} + y_4y_{15} + y_6y_{15} + y_8y_{15} + y_3y_{16} + y_5y_{16} + y_7y_{16}.
\end{aligned}$$

Simply applying Lemma 6 the system gets way easier:

$$\begin{aligned}
&Y_1 + Y_3 + Y_7 + Y_9 + Y_{10} + Y_{11} + Y_{12} + Y_{13} + Y_{14},\\
&Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_7 + Y_8 + Y_9 + Y_{10} + Y_{13},\\
&\vdots\\
&Y_0 + Y_3 + Y_5 + Y_7 + Y_9 + Y_{10} + Y_{13} + Y_{14},\\
&Y_0 + Y_1 + Y_3 + Y_4 + Y_5 + Y_6 + Y_9 + Y_{11} + Y_{13}.
\end{aligned}$$

Writing down, for example, p_{14} (second to last one) in a dense representation we get:

$$1{\cdot}Y_0{+}0{\cdot}Y_1{+}0{\cdot}Y_2{+}1{\cdot}Y_3{+}0{\cdot}Y_4{+}1{\cdot}Y_5{+}0{\cdot}Y_6{+}1{\cdot}Y_7{+}0{\cdot}Y_8{+}1{\cdot}Y_9{+}1{\cdot}Y_{10}{+}0{\cdot}Y_{11}{+}0{\cdot}Y_{12}{+}1{\cdot}Y_{13}{+}1{\cdot}Y_{14}.$$

Reading off the corresponding coefficient vector we get exactly the 14th row of T:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

4 Conclusion

In this paper we have shown a full break of the Hidden Irreducible Polynomials scheme introduced by Gómez in [1]. We have shown that the private key is publicly known by the design of the system. Moreover, we have shown that due to the construction of the private map, namely univariate polynomial multiplication, one can even easily read off the transformation matrix for the system of multivariate quadratic polynomial equations such that not even linear algebra is needed for attacking the scheme.

References

[1] Borja Gómez. Hidden irreducible polynomials : A cryptosystem based on multivariate public key cryptography. Cryptology ePrint Archive, Report 2019/1174, 2019.

[2] Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'99, pages 206–222, Berlin, Heidelberg, 1999. Springer-Verlag.

[3] T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88*, pages 419–453, New York, NY, USA, 1988. Springer-Verlag New York, Inc.

[4] Jacques Patarin. Cryptoanalysis of the matsumoto and imai public key scheme of eurocrypt'88. In *Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '95, pages 248–261, Berlin, Heidelberg, 1995. Springer-Verlag.

[5] Jacques Patarin. Hidden fields equations (hfe) and isomorphisms of polynomials (ip): Two new families of asymmetric algorithms. In *Proceedings of the 15th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'96, pages 33–48, Berlin, Heidelberg, 1996. Springer-Verlag.

[6] Jacques Patarin, Nicolas Courtois, and Louis Goubin. Flash, a fast multivariate signature algorithm. In *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA*, CT-RSA 2001, pages 298–307, Berlin, Heidelberg, 2001. Springer-Verlag.