CRYPTANALYSIS OF $\mathcal{HFE}$

ILIA TOLI

Abstract. Out of the public key ($\mathcal{PK}$) we recover a polynomial of the same degree as the private polynomial. This fact puts an eavesdropper in the same position with a legitimate user in decryption. The complexity of that all is $\mathcal{O}(d^3)$, for d an upper bound of the degree of the private polynomial.

1. Introduction

The problem of solving systems of multivariate polynomial equations is a well-known hard problem. In complexity theory, it is well-known to be an $\mathcal{NP}$-complete problem. Furthermore, even if we limit ourselves to the problem of solving systems of multivariate polynomial of degree two equations, we have again an $\mathcal{NP}$-complete problem. Therefore, it has been paid a lot of attention, since the invention of the idea of the pubic key cryptography, by Diffie and Hellman [DH76].

A lot of cryptosystems have been proposed since then, where an eavesdropper is asked to accomplish the hard task of solving systems of quadratic equations. However, most of them had short lives. The information that an eavesdropper had on the shape of the private key usually sufficed to render eavesdropping quite accesible. Some of their cryptanalyses aimed to recover the private key, or something equivalent, in the sense that gives the same privileges. Other cryptanalyses reduce the problem to accessible exhaustive searches, and so on.

In this paper we concentrate on $\mathcal{HFE}$. It is a $\mathcal{PK}$ cryptosystem first proposed by Patarin [Pat96]. In its main version, its $\mathcal{PK}$ is a system of n quadratic polynomial equations in n variables with coefficients in a finite field $\mathbb{F}_q$, practically $\mathbb{F}_2$. Its private key is:

- a basis, up to an isomorphism, of an overfield $\mathbb{K} \supset \mathbb{F}_q$, $[\mathbb{K} : \mathbb{F}_q] = n$, as an $\mathbb{F}_q$-vector space;
- a univariate polynomial f of a certain form, with coefficients in $\mathbb{K}$;
- two affine transformations of $\mathbb{K}$.

In the our cryptanalysis we find another polynomial of the same degree with f, such that its knowledge would put an eavesdropper in the same position as a legitimate user on recovering cleartexts. All of this

1991 *Mathematics Subject Classification.* Primary: 11T71; Secondary: 12H05.
Key words and phrases. Public key, hidden monomial, $\mathcal{HFE}$, $\mathcal{HPE}$.

task can be performed within $\mathcal{O}(d^3)$ bit operations, where $d = \deg f$. The degree of the extension n is practically of no importance to an eavesdropper.

2. The Cryptosystem

Let the parties committed to the tasks be:

- Alice who wants to receive secure messages;
- Bob who wants to send her secure messages;
- Eve, the eavesdropper.

Alice chooses two finite fields $\mathbb{F}_q < \mathbb{K}$, and a basis $\beta_1, \beta_2, \ldots, \beta_n$ of $\mathbb{K}$ as an $\mathbb{F}_q$-vector space. In practice, $q = 2$. However, it can be any p^r, for any p prime, and any $r \in \mathbb{N}$.

Next she takes a univariate polynomial of the form:

$$f(x) = \sum_{i,j} \gamma_{ij} x^{q^{\theta_{ij}} + q^{\varphi_{ij}}} + \sum_i \alpha_i x^{q^{\xi_i}} + \mu_0, \tag{1}$$

with coefficients in $\mathbb{K}$, and two affine transformations: $\mathcal{S}, \mathcal{T} : \mathbb{K} \to \mathbb{K}$; one left, one right.

With manipulations that we skip in order to save space, she generates her public key, a set of n quadratic polynomials of degree two, in n variables. The interested reader can find details in [IM85, IM89, hfe, Tol03]. Her private key is:

- the basis B of $\mathbb{K}$ as an $\mathbb{F}$-vector space;
- $\mathcal{S}$, $\mathcal{T}$, f.

3. The Cryptanalysis

Let Eve fix the canonical basis of $\mathbb{K}$. She may assume to apply a nondegenerate linear transformation $\mathcal{L}$ to the private basis B of $\mathbb{K}$, and to f. So, she obtains the canonical basis of $\mathbb{K}$, and another polynomial f_1, of the same form and degree like f.

Next, applying affine transformations $\mathcal{S}$, $\mathcal{T}$ to f_1 does not change its degree. If it werent for the last translation, the public polynomial $\mathcal{S} \circ f \circ \mathcal{L} \circ \mathcal{T}$ is even of the same form like the polynomial f.

Alice has limitation on taking $d = \deg f$. Her decryption becomes exponentially harder with its growth. Besides, if it is big, the number undesired solutions grows a lot. To discard them, she introduces other, randomly chosen polynomials. This renders the public key overdefined. So, the cryptosystem becomes particularly weak to certain attacks.

So, Eve may assume d bounded. She fixes a bound of it. Next, she writes down the general polynomial of degree d:

$$A_d x^d + A_{d-1} x^{d-1} + \cdots + A_1 x + A_0. \tag{2}$$

Nex, Eve has only to do $d + 1$ evaluations of the public key. So, she obtains a linear system of $d + 1$ equations in the $d + 1$ variables A_i.

Solving it enables Eve to recover $\mathcal{S} \circ f \circ \mathcal{L} \circ \mathcal{T}$ in the form of a univariate polynomial with coefficients in $\mathbb{K}$.

So, Eve is already in the same position with Alice in decryption. With another calculus of no comutational effort, she can render her polynomial even sparse, as much as possible.

Indeed, if d is the degree of the polynomial that she recovers, much probably $d-1$ does not qualify to be a power of a monomial of a polynomial of the form (1). If this is the case, the shift is: $x - \frac{A_{d-1}}{A_d}$. Otherwise, the shift is easy to calculate, anyway, and anyway is not essential to make Eve be at the same position as Alice in decryption.

4. A Variation that Would Resist such an Attack

So, the main flaw of $\mathcal{HFE}$ is the bounded degree of its private polynomial. Here is a variation that seems to resist such an attack.

Alice takes an affine polynomial f of any degree. She generates her set of polynomials upon the polynomial $f^2 \bmod (x^{q^n} - x)$. This polynomial is of the same form as (1), and does not have bound on degree. So, the previous attack does not work.

In decryption, Alice calculates the square roots of the ciphertext, and then has to solve a univariate affine polynomial equation on its suqare roots.

References

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. In *IEEE Trans. Information Theory*, pages 644–654, 1976. http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf.

[hfe] http://www.minrank.org/hfe/ or http://www.hfe.info/.

[IM85] Hideki Imai and Tatsuo Matsumoto. Algebraic methods for constructing asymmetric cryptosystems. In *Algebraic Algorithms and Error-Correcting Codes, Proceedings Third International Conference*, pages 108–119, Grenoble, France, 1985. Springer-Verlag.

[IM89] Hideki Imai and Tatsuo Matsumoto. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Advances in Cryptology, Eurocrypt '88*, pages 419–453. Springer-Verlag, 1989. http://link.springer.de/link/service/series/0558/papers/0330/03300419.pdf.

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. *Lecture Notes in Computer Science*, 1070:33–on, 1996. http://www.minrank.org/hfe.pdf.

[Tol03] Ilia Toli. Hidden polynomial cryptosystems. Cryptology ePrint Archive, Report 2003/061, 2003. http://eprint.iacr.org/2003/061.pdf.

Dipartimento di Matematica *Leonida Tonelli*, via F. Buonarroti 2, 56127 Pisa, Italy., toli@posso.dm.unipi.it